EXHIBIT C
Part 2 of 3

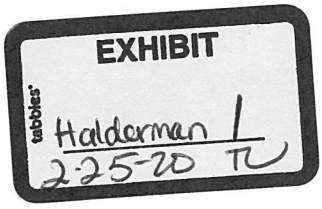
IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FAIR FIGHT ACTION, INC., *et al.*, Plaintiffs v. BRAD RAFFENSPERGER, in his official Capacity as Secretary of State of Georgia; *et al.*, Defendants.	Civil Action File No. 1:18-cv-05391-SCJ

DEFENDANTS' AMENDED NOTICE TO TAKE THE EXPERT DEPOSITION OF J. ALEX HALDERMAN, Ph.D.

PLEASE TAKE NOTICE that, pursuant to Rule 30 of the Federal Rules of Civil Procedure, counsel for Defendants Brad Raffensperger, et al., will take the deposition upon oral examination of Plaintiff Fair Fight Action, Inc.'s expert, J. Alex Halderman, Ph.D. The deposition will take place at the Delta Detroit Metro Airport Hotel, 31500 Wick Road, Romulus, MI 48174, on Tuesday, February 25, 2020, beginning at 9:30 a.m. and continuing thereafter until completed.

The deposition will be taken before a notary public or other officer authorized to administer oaths for purposes of discovery, cross-examination, and all other purposes authorized by law. It will be recorded by stenographic and/or video means.



This 11th day of February, 2020.

/s/ Bryan P. Tyson
Bryan P. Tyson
Special Assistant Attorney General
Georgia Bar No. 515411
btyson@taylorenglish.com
Bryan F. Jacoutot
Georgia Bar No. 668272
bjacoutot@taylorenglish.com
Diane F. LaRoss
Georgia Bar No. 430830
dlaross@taylorenglish.com
Taylor English Duma LLP
1600 Parkwood Circle - Suite 200
Atlanta, Georgia 30339
Telephone: (678) 336-7249

Josh B. Belinfante
Georgia Bar No. 047399
jbelinfante@robbinsfirm.com
Vincent R. Russo
Georgia Bar No. 242628
vrusso@robbinsfirm.com
Brian E. Lake
Georgia Bar No. 575966
blake@robbinsfirm.com
Carey A. Miller
Georgia Bar No. 976240
cmiller@robbinsfirm.com
Alexander Denton
Georgia Bar No. 660632
adenton@robbinsfirm.com
Robbins Ross Alloy Belinfante Littlefield LLC
500 14th Street, N.W.
Atlanta, Georgia 30318
Telephone: (678) 701-9381
Facsimile: (404) 856-3250

Christopher M. Carr
Attorney General
GA Bar No. 112505
Annette M. Cowart
Deputy Attorney General
GA Bar No. 191199
Russell D. Willard
Senior Assistant Attorney General
GA Bar No. 760280
State Law Department
GA Bar No. 760280
40 Capitol Square, S.W.
Atlanta, Georgia 30334

Attorneys for Defendants

CERTIFICATE OF SERVICE

I hereby certify that, on February 11, 2020, I caused to be served the foregoing **DEFENDANTS' AMENDED NOTICE TO TAKE THE EXPERT DEPOSITION OF J. ALEX HALDERMAN, Ph.D.** by email to the following:

Lawrence & Bundy LLC
Allegra Lawrence-Hardy
Leslie J. Bryan
Maia J. Cogen
Suzanne Smith Williams
1180 West Peachtree Street, NW
Suite 1650
Atlanta, GA 30309
Allegra.Lawrence-Hardy@lawrencebundy.com
Leslie.Bryan@lawrencebundy.com
Maia.Cogen@lawrencebundy.com
Suzanne.Williams@lawrencebundy.com

KaiserDillon PLLC
Matthew G. Kaiser
Sarah R. Fink
Scott S. Bernstein
Norman G. Anderson
1099 14th Street, NW
8th Floor West
Washington, DC 20005
mkaiser@kaiserdillon.com
sfink@kaiserdillon.com
sbernstein@kaiserdillon.com
nanderson@kaiserdillon.com

Lawrence & Bundy, LLC
Thomas R. Bundy
8115 Maple Lawn Blvd.
Suite 350
Fulton, MD 20759
Thomas.Bundy@lawrencebundy.com

Sandler Reiff Lamb Rosenstein & Birkenstock, P.C.
Dara Lindenbaum
1090 Vermont Ave, NW
Suite 750
Washington, DC 20005
lindenbaum@sandlerreiff.com

Elizabeth Vranicar Tanis
John A. Chandler
957 Springdale Road, N.E.
Atlanta, GA 30306
beth.tanis@gmail.com
jachandler@gmail.com

Kastorf Law, LLC
Kurt G. Kastorf, Esq,
1387 Iverson Street NE
Suite 100
Atlanta, GA 30307
kurt@kastorflaw.com

Jenner & Block LLP
Kali Nneka Bracey
1099 New York Avenue, NW
Suite 900
Washington, DC 20001
KBracey@jenner.com

Jenner & Block LLP
Jeremy H. Ershow
919 Third Avenue
New York, New York 10022
jershow@jenner.com

Miller & Chevalier Chartered
Andrew D. Herman
Nina C. Gupta
900 16th St. NW
Washington, DC 20006
aherman@milchev.com
ngupta@milchev.com

DuBose Miller LLC
Von A. DuBose
75 14th Street N.E., Suite 2110
Atlanta, GA 30309
dubose@dubosemiller.com

/s/ Bryan P. Tyson
Bryan P. Tyson
Georgia Bar No. 515411

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FAIR FIGHT ACTION, et al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	Civ. Action No. 1:18-cv-05391-SCJ
	)	
BRAD RAFFENSPERGER, in his official capacity as Secretary of State of the State of Georgia, et al.,	)	
	)	
Defendants.	)	

EXPERT REPORT OF J. ALEX HALDERMAN

Professor of Computer Science & Engineering
Director, University of Michigan Center for Computer Security and Society
University of Michigan
Beyster Building, Room 4717
2260 Hayward Street
Ann Arbor, MI 48109-2121

February 18, 2020

J. Alex Halderman, Ph.D.
[signature to be supplied]

EXPERT REPORT OF J. ALEX HALDERMAN, Ph.D.

1. My name is J. Alex Halderman.

2. My background, qualifications, and professional affiliations are set forth in my curriculum vitae, which is attached as Exhibit A.

3. I hold a Ph.D. (2009), a master's degree (2005), and a bachelor's degree (2003), *summa cum laude*, in computer science, all from Princeton University.

4. I am Professor of Computer Science and Engineering, Director of the Center for Computer Security and Society, and Director of the Software Systems Laboratory at the University of Michigan in Ann Arbor, Michigan.

5. My research focuses on computer security and privacy, with an emphasis on problems that broadly impact society and public policy. Among my areas of research are software security, network security, and election cybersecurity.

6. I serve as co-chair of the State of Michigan's Election Security Advisory Commission, by appointment of the Michigan Secretary of State.

7. I have testified before the U.S. Senate Select Committee on Intelligence and before the U.S. House Appropriations Subcommittee on Financial Service and General Government on the subject of cybersecurity and U.S. elections.

8. I have performed security testing of electronic voting systems for the Secretary of State of California.

9. I have authored more than 85 articles and books. My work has been cited in more than 9,400 scholarly publications. I have served on the program committees for 33 research conferences and workshops. I co-chaired the USENIX Election Technology Workshop, which focuses on electronic voting security.

10. I have published numerous peer-reviewed research papers analyzing the security of electronic voting systems used in U.S. states and in other countries. I have also investigated methods for improving election security, such as efficient techniques for auditing whether computerized election results match paper ballots.

11. I regularly teach courses in computer security, network security, and election cybersecurity at the graduate and undergraduate levels. I am the creator of *Securing Digital Democracy*, a massive, open, online course about computer security and elections that has attracted more than 20,000 students.

12. I received the John Gideon Award for Election Integrity from the Election Verification Network, the Andrew Carnegie Fellowship, the Alfred P. Sloan Foundation Research Fellowship, the IRTF Applied Networking Research Prize, the Eric Aupperle Innovation Award, the University of Michigan College of Engineering 1938 E Award for teaching and scholarship, and the University of Michigan President's Award for National and State Leadership.

13. I am being compensated for my work related to this matter at my customary rate of $750 per hour. My compensation does not depend on the outcome of this litigation, the opinions I express, or the testimony I provide.

Georgia's Election Technology

14. Plaintiffs have asked me to opine on the security of Georgia's election system following the implementation of new technology from Dominion Voting Systems, Inc. ("Dominion") and KNOWiNK, LLC ("KnowInk"). The state is in the process of deploying Dominion ImageCast X Prime ("ICX") ballot marking devices (BMDs), ImageCast Precinct ("ICP") precinct-count scanners, ImageCast Central ("ICC") central-count scanners, the Democracy Suite election management system (EMS), and KnowInk Poll Pad electronic poll books. Georgia Secretary of State Brad Raffensperger certified the Dominion components in August 2019.[1]

15. I have reviewed documents provided by Dominion in response to a subpoena from Plaintiffs. These documents include technical documentation about the election system components, the company's response to Georgia's Request for Proposals for the new voting system, reports from third-party testing, and certain internal engineering memos relating to the security of the system.

[1] Georgia Dominion/KnowInk certification (Aug. 9, 2019), https://sos.ga.gov/admin/uploads/Dominion_Certification.pdf.

16. I understand that Georgia maintains its voter registration database using a system called ElectioNet ("eNet"), which was developed and is maintained by PCC Technology, Inc. Election officials use eNet to manage voter registration data and to export it to electronic poll books for each election. The Georgia My Voter Page (MVP) and Online Voter Registration (OVR) websites interface with eNet and allow voters to view and update their voter registration data. At each polling place, workers use Poll Pad electronic poll books to check in voters. The Poll Pads consist of off-the-shelf Apple iPads running custom software. The Poll Pads are also used to program "voter cards," which the voter uses to activate a ballot marking device and begin a voting session.

17. Georgia plans for all in-person voters to select candidates using Dominion ICX BMDs, which are computer tablets connected to off-the-shelf laser printers. These devices do not record votes but instead print paper ballots that are supposed to contain the voter's selections in both human-readable text and as a type of machine-readable barcode called a QR code. The voter will insert the paper ballot into a Dominion ICP optical scanner, which will store a digital scan of the printout. The scanner will process the barcode and count the votes encoded in it, and the paper ballots will be retained for use in audits or recounts. Absentee voters will not use

BMDs but will instead complete hand-marked paper ballots (HMPBs), which will be tabulated at central locations by Dominion ICC optical scanners.

18. Before every election, the Secretary of State's office will prepare election programming files using the Dominion EMS software, which is a collection of client and server programs that run on commercial-off-the-shelf (COTS) computers and servers. The Secretary of State will transmit the election programming files to county officials, who will use another instance of the Dominion EMS to prepare memory cards and USB sticks for every scanner and ballot marking device used in the county. These removable media will contain the ballot design, including the names of the races and candidates, and rules for counting the ballots. Election workers will install a memory card or USB stick into each BMD and ICP scanner prior to the start of voting.

19. After polls close, election workers will remove the memory cards from every ICP scanner and return them to the county. At that point, the memory cards will contain a digital image of each scanned ballot as well as the scanner's interpretation of the votes each ballot contains. County workers will use the Dominion EMS to retrieve data from the cards and prepare the final election results.

Threats to Georgia Elections

20. In my opinion, Georgia's election system faces a high risk of being targeted by sophisticated adversaries, including Russia and other hostile foreign governments. These adversaries could attempt to hack the election system to achieve a variety of goals, including undermining voter confidence and causing fraudulent election outcomes. Attackers could sabotage BMDs or optical scanners to prevent them from functioning on election day, or to cause obviously incorrect results. They could also infiltrate BMDs and scanners with malicious software in order to cause plausible but fraudulent election results. As I will explain, attacks by sophisticated attackers such as foreign governments could succeed despite procedural and technical protections that Georgia has in place, including a paper trail and limited post-election audits.

21. The Mueller Report outlined the scale and sophistication of Russia's efforts to interfere in the 2016 election, leaving no doubt that Russia and other adversaries will strike again.[2] The Special Counsel concluded principally that "[t]he Russian government interfered in the 2016 presidential election in sweeping and

[2] Special Counsel Robert S. Mueller, III *Report on the Investigation into Russian Interference in the 2016 Presidential Election (Volume I of II)*, United States Department of Justice (Mar. 2019), https://www.justice.gov/storage/report.pdf.

systematic fashion."[3] The report further explained that foreign actors "sought access to state and local computer networks by exploiting known software vulnerabilities on websites of state and local governmental entities."[4] The report also found that these foreign agents were successful in attacking at least one state and that their activities involved "more than two dozen states."[5] As noted prior to the Special Counsel's final report, Georgia was among the states that Russia targeted.[6]

22. Russia has sophisticated cyber-offensive capabilities, and it has shown a willingness to use them to hack elections elsewhere even before 2016. For instance, according to published reports, during the 2014 presidential election in Ukraine, attackers linked to Russia sabotaged Ukraine's vote counting infrastructure, and Ukrainian officials succeeded only at the last minute in defusing vote-stealing malware that would have caused the wrong winner to be announced.[7] Other adversarial governments have similarly advanced cyberwarfare capabilities, including China, Iran, and North Korea, and might target future Georgia elections.

---

[3] *Id.* at 1.
[4] *Id.* at 50.
[5] *Id.*
[6] *See* Indictment ¶ 75, *United States v. Netyksho*, No. 1:18-cr-00215-ABJ, , (D.D.C. July 13, 2018), ECF No. 1.
[7] Mark Clayton, "Ukraine election narrowly avoided 'wanton destruction' from hackers," *The Christian Science Monitor* (June 17, 2014), https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.

23. It is my opinion that Georgia's new voting technology does not achieve the level of security necessary to withstand an attack by a sophisticated adversary such as a hostile foreign government. Despite the addition of a paper trail, it suffers from serious security risks much like those of the paperless voting system it has replaced. Attackers can potentially subvert the election technology in several ways:

(a) Attackers could infiltrate the voter registration database and extract, change, or erase voter registration records. These attacks could cause voters to receive the wrong ballot or be prevented from casting a regular ballot. They could also be used to steal information that could be used to impersonate voters.

(b) Attackers could sabotage polling place equipment, including Poll Pads, BMDs, and ICP scanners, and prevent them from functioning on election day. This would cause lengthy delays and drive away many eligible voters. An attacker could target such sabotage at jurisdictions that strongly favored a particular candidate and thereby cause a partisan shift in the election outcome.

(c) Attackers could manipulate optical scanners or election management systems to cause them to report fraudulent outcomes. Attacks on the scanners could alter all digital records of the election results. The only

kind of safeguard that can reliably detect such an attack is a sufficiently rigorous manual audit or recount of the paper ballots, which Georgia does not currently require.

(d) Attackers could infiltrate the BMDs to cause them to sometimes print ballots that differ from voters' on-screen selections. Such an attack might change only the ballot barcode, which is the only portion of the ballot that the scanners count. The change would be invisible to voters. Unless all races are rigorously audited by inspecting the human-readable portion of the paper ballots, such attacks could go undetected.

(e) Attackers could also infiltrate the BMDs and change both the barcode *and* the human-readable text on some of the ballots. Research shows that few voters carefully review their printed ballots, and consequently fraud sufficient to change the winner of a close race might go undetected. No audit or recount could detect the change, since both the digital and paper records would be wrong.

24. One way that attackers could carry out these attacks is by introducing malicious software ("malware") into the election equipment. Malware could be introduced in several ways, including: (a) with physical access to the equipment, (b) by dishonest election workers, (c) through an attack on the hardware or software

supply-chain, or (d) by spreading from the election management systems to polling place equipment during routine pre-election procedures.

25. Critical components of Georgia's election system are directly connected to the Internet. These include the eNet voter registration system, the Georgia My Voter Page (MVP) and Online Voter Registration (OVR) websites, and the Poll Pad electronic poll books. Being connecting to the Internet exposes these systems to the threat that attackers anywhere in the world could directly target them.

26. Other components of Georgia's election system that are not directly connected to the Internet might nonetheless be targeted by attackers. Nation-state attackers have developed a variety of techniques for infiltrating non-Internet-connected systems, including by spreading malware on removable media that workers use to copy files in and out.[8] Attackers could employ this method to infect the state or county EMS and spread from there to scanners and BMDs when workers program them for the next election. In this way, an attack could potentially spread

[8] A well-known example of this ability, which is known as "jumping an air gap," is the Stuxnet computer virus, which was created to sabotage Iran's nuclear centrifuge program by attacking factory equipment that was not directly connected to the Internet. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired* (Nov. 3, 2014), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

form a single point of infection to scanners and BMDs across entire counties or the whole state.

Vulnerabilities in Georgia Voting Equipment

27. **Dominion components.** Dominion does not dispute that its devices can be hacked by sufficiently sophisticated adversaries.[9]

28. One reason why this is true is the complexity of the software. The Dominion software used in Georgia contains nearly 2.75 million lines of source code (equivalent to about 45,000 printed pages), excluding the Windows and Android operating systems and other off-the-shelf software packages.[10] The ICP scanner alone contains about 475,000 lines of source code, and its software is written in C/C++,[11] a programming language that is particularly susceptible to some of the most dangerous types of vulnerabilities.

29. Software of the size and complexity of the Dominion code inevitably has exploitable vulnerabilities. As a code review team working for the California

---

[9] Decl. of Dr. Eric Coomer, Director of Product Strategy and Security for Dominion ¶ 13, *Curling v. Raffensperger*, No 1:17-cv-2989-AT (N.D. Ga. Nov. 13, 2019), ECF No. 658-2 ("all computers can be hacked with enough time and access").

[10] SLI Compliance, "Dominion Democracy Suite 5.10 Voting System Software Test Report for California Secretary of State" 6 (Aug. 2019), https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510software-report.pdf.

[11] *Id.*

Secretary of State concluded in a study of a voting system with only 10% as much code as Dominion's, "If the [system] were secure, it would be the first computing system of this complexity that is fully secure."[12] Nation-state attackers often discover and exploit novel vulnerabilities in complex software.[13]

30. In addition to its complexity, the Dominion software utilizes a wide range of outdated off-the-shelf software modules, including some that perform essential security functions, such as the operating system and modules that process files an attacker might have manipulated.[14] The oldest third-party software components appear not to have been updated in more than 15 years. Old or outdated software used in Georgia's new Dominion equipment includes a version of Microsoft SQL Server dating from 2016, Adobe Acrobat from around 2015, barcode scanner software from 2015, Android operating system software from 2015, µClinux

---

[12] Joseph A. Calandrino, Ariel J. Feldman, J. Alex Halderman, David Wagner, Harlan Yu, and William Zeller, "Source Code Review of the Diebold Voting System," in *California Secretary of State's Top-to-Bottom Review of Voting Systems* (July 20, 2007), https://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-source-public-jul29.pdf.

[13] Andrew Springall, *Nation-State Attackers and their Effects on Computer Security* (2009), Ph.D. dissertation, University of Michigan, https://deepblue.lib.umich.edu/handle/2027.42/143907.

[14] SLI Compliance, "Dominion Voting Systems Democracy Suite 5.5-A Certification Test Plan" 16-19 (Dec. 2018), https://www.eac.gov/sites/default/files/voting_system/files/DVS_Democracy_D-Suite_5.5-A_Modification_Test_Plan_v1.2.pdf.

operating system software from 2007, COLILO bootloader software from 2004, and a version of the Apache Avalon component framework dating from 2002.

31. Outdated software components are a security risk because they frequently contain known, publicly documented vulnerabilities that have been corrected in later versions. For example, the version of the Android operating system used Georgia's ICX BMDs, Android 5.1.1, contains 254 known vulnerabilities.[15]

32. Dominion's response to Georgia's RFP lists among "key personnel" a "Chief Security Officer" (CSO) whose responsibilities for the voting system project will be "Oversight of key security development and implementation."[16] However, at the time of the RFP, the CSO position was vacant, and to my knowledge Dominion has yet to fill the role. It is unclear who at Dominion has responsibility for security development and implementation in the context of the Georgia components.

33. Georgia certified the Dominion system without performing its own security testing or source code review. The certification was preceded by tests performed that were limited to checking functional compliance with Georgia

[15] CVE Details, "Google Android 5.1.1 Security Vulnerabilities," https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/-version_id-186573/Google-Android-5.1.1.html (last visited Feb. 10, 2020).
[16] DOM-003996.

requirements.[17] The test report states that the testing "was not intended to result in exhaustive tests of system hardware and software attributes."[18] The word "security" does not appear in the report.

34. At around the same time that Georgia certified the Dominion system, California performed tests on a more recent version of the Dominion software (version 5.10) as part of its own certification process.[19] In contrast to Georgia's tests, California's did include some source code review and security testing.

35. Like all security testing, the California tests were necessarily limited in scope and could not be expected to find all exploitable vulnerabilities. Nevertheless, they did uncover several serious flaws. In my experience, more recent versions of software tend to contain fewer security vulnerabilities than older versions, and so these problems very likely apply to the Georgia version of the Dominion system.

36. The California testers found that attackers could modify the Dominion software installation files and believed that "it would be possible to inject more lethal

---

[17] Pro V&V, "Test Report: Dominion Voting Systems D-Suite 5.5-A Voting System Georgia State Certification Testing" (Aug. 7, 2019), https://sos.ga.gov/admin/uploads/Dominion_Test_Cert_Report.pdf.

[18] *Id.* at 3.

[19] SLI Compliance, "Dominion Democracy Suite 5.10 Security and Telecommunications Test Report" (Aug. 2019), https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510security-report.pdf ("California Certification Security and Telecomm Test Report").

payloads into the installers given the opportunity."[20] This implies that attackers could modify the Dominion installation files to infect election system components with malicious software.

37. Furthermore, the California testers found that the Dominion system's antivirus protection was insufficient or non-existent. "[O]n the EMS server, the AVAST Antivirus (AV) File Shield (the real time AV monitor) was only able to detect and clean one of the four [test] files. This potentially leaves the system open to zipped and double zipped viruses as well as infection strings in plain text."[21] Moreover, the ICX BMD and ICP optical scanner have no antivirus software at all.[22] As a result, malware that infected the Dominion components could evade antivirus detection.

38. One way that attackers might affect election equipment is by physically accessing the devices. In the case of the BMD, the California source code reviewers found a vulnerability that can be exploited with physical access to the USB port that "would be open to a variety of actors including a voter, a poll worker, an election official insider, and a vendor insider."[23] This implies that no secret passwords or

---

[20] *Id.* at 25.
[21] *Id.* at 19-20.
[22] *Id.* at 20.
[23] California Secretary of State's Office of Voting Systems Technology Assessment, "Dominion Voting Systems Democracy Suite 5.10 Staff Report" 29

keys would be needed to exploit the problem, given physical access. California testers also found that "the ICX device does not provide monitoring of physical security,"[24] and that, for all the polling place devices, including the ICX, "[s]ecurity seals, locks, and security screws can be circumvented."[25]

39. Other weaknesses found in the California tests include that "a number of passwords were able to be recovered that were stored in plain text,"[26] that the network switch used to connect EMS clients and servers was "determined to have twelve medium vulnerabilities and four low vulnerabilities,"[27] and that, if an authentication device used by poll workers and administrators was lost or stolen shortly before an election, revoking its access would require a logistically difficult process to reprogram the election files for the polling place devices.[28] These problems indicate that the Dominion system was designed without sufficient attention to security.

(Aug. 19, 2019), https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510staff-report.pdf.

[24] California Certification Security and Telecomm Test Report at 11.

[25] *Id.* at 17.

[26] *Id.* at 15.

[27] *Id.* at 30.

[28] *Id.* at 15.

40. Although California ultimately permitted the Dominion system to be used, its certification requirements impose much more stringent security conditions than those in Georgia.[29]

41. **Voter registration components.** Georgia has used the eNet voter registration database system for many years. I understand that the state commissioned a vendor cyber risk assessment of eNet in February 2018. The assessment encompassed a contract and documentation review, network scans and reviews of server configurations, and interviews with key personnel at PCC, the vendor that developed and (at the time) operated eNet. The assessment was limited in scope and did not include source code review or penetration testing. Even this limited review identified serious security deficiencies in both the software and PCC's network environment. In July 2019, the Secretary of State assumed operational responsibility for eNet, but development and maintenance of the software continue to be the responsibility of PCC.

42. Transferring eNet operations to the Secretary of State's office does not mitigate the full range of issues that the State's experts identified, and there is no evidence that the State has taken other steps to address them. Moreover, the 2018

[29] California Secretary of State, "Conditional Approval of Dominion Voting Systems, Inc. Democracy Suite Version 5.10 Voting System" (Oct. 18, 2019), https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds510-cert.pdf.

security assessment was of limited scope, and a more thorough assessment, including a source code review and penetration tests, would be necessary to ensure that all relevant issues are discovered and corrected.

43. The Georgia My Voter Page (MVP) and Online Voter Registration (OVR) websites that interface with eNet provide another avenue by which attackers could attempt to infiltrate the voter registration system. Serious vulnerabilities in the MVP website were discovered on the eve of the November 2018 election and reported to the Secretary of State. Unauthorized parties could have exploited these vulnerabilities to access sensitive system configuration files and voter registration data. This information would have allowed attackers to fraudulently change voters' registrations through the OVR system. Cursory security testing should have uncovered the MVP vulnerabilities, and their existence calls into question the overall security of the MVP and OVR websites.

44. **Electronic poll books.** The Poll Pads electronic poll books communicate with an Internet-based administration system called ePulse. Election workers use the ePulse website to upload lists of eligible voters for each precinct, manage Poll Pad devices, and retrieve voter history data after an election. When polls are open, Poll Pads can be configured in a fully connected mode, in which they continuously communicate with ePulse over the Internet, or in a peer-to-peer

communication mode, in which they exchange data with other Poll Pads in the polling place over a Bluetooth or WiFi wireless network.

45. Internet access and wireless capabilities expose the Poll Pads to a large variety of security risks. If attackers are able to infiltrate ePulse, they could remotely alter voter registration data before it is downloaded by the Poll Pads, or they could potentially spread malicious software to the Poll Pads. Attackers could also likely exploit the devices' wireless capabilities to disable Poll Pads during voting.

46. To my knowledge, Georgia has not performed any security testing of the Poll Pad electronic poll books. In contrast, the Secretary of State of California commissioned source code review[30] and penetration testing[31] of the Poll Pad in 2018. Among several significant deficiencies found by California were: (i) cross-site scripting vulnerabilities and insecure use of HTTP Cookies in the ePulse website, which could allow attackers to hijack election officials' accounts; (ii) the ability of the software to delete log files without this action itself being logged, which could

[30] SLI Compliance, "KNOWiNK PollPad Plus 1.0 Electronic Poll Book System Source Code Review Test Report for California" (May 6, 2018), https://votingsystems.cdn.sos.ca.gov/vendors/knowink/source-code-report.pdf.
[31] SLI Compliance, "KNOWiNK PollPad Plus 1.0 Electronic Poll Book System Security and Telecommunications Test Report for California" (May 11, 2018), https://votingsystems.cdn.sos.ca.gov/vendors/knowink/security-report.pdf.

help attackers hide evidence of their activities; and (iii) improper programming structures that apparently created the potential for inadvertent data loss.

47. Following these tests, California conditionally certified the Poll Pad subject to 19 terms and limitations that reflect the findings of the security testing.[32] Among the conditions is that Poll Pads may not be connected to smart card encoders, which ensure that there is no path for an attack to spread from the Poll Pads to BMDs.

48. Pennsylvania also evaluated and conditionally certified the Poll Pad in 2018.[33] The Pennsylvania certification is subject to 24 conditions and accompanied by five additional security recommendations. The conditions include that Poll Pads must not be configured to communicate with ePulse over the Internet during polling, and that Poll Pads and their removable media must never be connected to other voting system components, including a prohibition of using the Poll Pads to encode voter access cards.

---

[32] California Secretary of State, "Conditional Approval of KnowInk, LLC PollPad Plus Version 1.0 Electronic Poll Book System" (May 22, 2018), https://votingsystems.cdn.sos.ca.gov/vendors/knowink/cert.pdf.

[33] Commonwealth of Pennsylvania Department of State, "Results of KnowInk Electronic Poll Book Poll Pad 1.3.3 Evaluation" (Oct. 5, 2018), https://www.dos.pa.gov/VotingElections/Documents/Voting%20Systems/Knowink%20PollPag%201.3.3/Knowink%20Poll%20Pad%201.3.3%20Approval%20Report.pdf.

49. It is unclear what conditions, if any, Georgia imposes on the use of Poll Pads. However, I understand that the Poll Pad will be used to encode voter activation cards that voters use with the Dominion BMDs. California and Pennsylvania both prohibit this functionality, as it creates a path by which an attack could spread from the Poll Pads (which have Internet access) to the BMDs.

50. **Supply chain threats.** In addition to the risk that external attackers will compromise Georgia election system components by exploiting software vulnerabilities, there is also a risk that attackers could infiltrate the software development process of Dominion, KnowInk, PCC, or their suppliers. By doing so, an adversary could steal source code or other secrets in order to more easily attack the election components. An attacker could also insert vulnerabilities or malicious functionality into the election system software during development.

51. Several critical components of the Dominion systems are designed and produced overseas. Much of the election software is programmed in Serbia, a country closely allied with Russia.[34] The EMS runs antivirus software made by a Czech company, which necessitates granting that software highly privileged access

[34] Patrick Thibodeau, "One election-system vendor uses developers in Serbia," *Computer World* (Oct. 5, 2016), https://www.computerworld.com/article/3126791/one-election-system-vendor-uses-developers-in-serbia.html.

to the EMS server. The ICX BMD runs on an Android-based tablet produced by a Taiwanese company. A hostile government might attempt to plant an agent at any of these companies, blackmail honest employees, or hack into the software development environments. Although multinational supply chains are common in the technology industry, they represent a heightened threat in election contexts due to foreign governments' military, diplomatic, and economic interests in U.S. election outcomes.

Intended Safeguards Provide Insufficient Protection

52. I understand that Georgia applies or intends to apply a variety of defenses within the election system. However, even when taken together, these defenses are insufficient to thwart attacks by sophisticated adversaries, such as hostile governments.

53. **AuditMark.** When the ICP and ICC scanners process a ballot, they generate a digital image of the ballot. A feature that Dominion calls "AuditMark" appends to the image a record of the scanner's interpretation of the votes. Election officials can later review the digital records of each ballot using the EMS.

54. Digital ballot images and the AuditMark feature do not secure the electronic vote records against tampering by malicious software. My own peer-reviewed research demonstrates how malware running on an optical scanner or EMS

could automatically manipulate digital ballot images to make them appear to support a different election result.[35]

55. For ballots that are marked by hand, malware can employ computer vision techniques to manipulate ballot images while preserving the voter's original marking style, so that the manipulated marks appear consistent with other marks on the ballot. Manipulation is even more straightforward when ballots are marked by a BMD, since the BMD prints all marks in a consistent style.

56. In either case, the tampering would not be detected by the election software and would be not be apparent to a human operator reviewing the ballot images and AuditMark data. The figure below shows an example of a Dominion-style ballot image that has been manipulated using the algorithm from our research:

---

[35] Matthew Bernhard, Kartikeya Kandula, Jeremy Wink, and J. Alex Halderman, "UnclearBallot: Automated Ballot Image Manipulation" in *Proceedings of the Fourth International Joint Conference on Electronic Voting* (Oct. 2019), https://jhalderm.com/pub/papers/unclear-evoteid19.pdf.

Original

County

Supervisor, District 1

	Vote for One
Alfred Hitchcock	◉
Vincent Price	○
Write In	○

State

Governor

	Vote for One
Amelia Earhart	○
Howard Hughes	⊗
Charles Lindbergh	○
Write In	○

Manipulated

County

Supervisor, District 1

	Vote for One
Alfred Hitchcock	○
Vincent Price	◉
Write In	○

State

Governor

	Vote for One
Amelia Earhart	⊗
Howard Hughes	○
Charles Lindbergh	○
Write In	○

Left: **Image of original Dominion-style voter-marked ballot.**

Right: **Image manipulated by malware to show fraudulent selections.**

57. **Hash comparisons.** I understand that Georgia may employ a method know an "hash comparison" to attempt to confirm that the correct software is installed on the EMS and polling place equipment. A "hash value" is a short numeric code that is calculated based on the contents of a file. The calculation method is designed so that it is difficult to figure out a way to modify the file without resulting in a different hash value. Officials might attempt to detect malware by comparing

the hash values of the software running in the election system to "known good" hash values calculated from a copy of the software that has not been altered by an attacker.

58. In response to Dominion's proposal for the election system, Georgia requested additional details about how a hash comparison can be performed during initial acceptance testing of the equipment, during pre-election processes, and immediately following an election. Dominion's responses[36] describe a hash comparison process that cannot reliably detect malicious changes to the machines.

59. There are separate comparison procedures for the EMS, ICX, ICP, and ICC. In each case, software on the equipment being tested is either responsible for calculating the hash value or for copying the files that are to be compared to removable media. If the equipment has been infected with malware, the malware could cause the machines to falsely compute the hash values of an uninfected system, or it could copy the original program files to the removable media while actually running a modified version of the files.

60. Furthermore, the hash comparisons described by Dominion for the cover only some of the software running on the devices. They fail to check the integrity of critical software such as the Windows and Android operating systems, as well as other programs and data files that could contain malware. These

[36] DOM-000143-49, 170-74, 210-11, and 239-42.

deficiencies provide multiple ways for a sophisticated attacker to conceal the presence of malware on the voting equipment even if officials practiced hash comparisons according to Dominion's instructions.

61. **Antivirus software.** As I have already described, California's security tests found that the antivirus software used on the Dominion EMS server was unable to detect some forms of malware, and that the ICP and ICX devices have no antivirus protection at all. In general, antivirus software and end-point protection software provide only a limited defense against sophisticated attackers like nation-states.

62. **Physical security.** I understand that one safeguard used in Georgia is tamper-evident seals. These seals are designed to indicate whether someone has opened the chassis of an optical scanner or BMD or accessed protected data ports or switches. Tamper evident seals do not protect against remote electronic attackers, and they provide only weak protection against attackers with physical access. The types of seals typically used for voting equipment can be bypassed without detection using readily available tools.[37] For some seals, these tools include screwdrivers and hair dryers. By bypassing the seals, an attacker with physical access to the polling place equipment can modify their internal programming and add malicious software.

[37] Andrew W. Appel, "Security Seals on Voting Machines: A Case Study," in *ACM Transactions on Information and System Security* (2011), https://www.cs.princeton.edu/~appel/voting/SealsOnVotingMachines.pdf.

63. **Logic and accuracy testing.** I understand that Georgia employs so-called "logic and accuracy" (L&A) testing. In L&A testing, officials cast a small number of ballots with known selections, then check whether the system's output reflects the correct votes. L&A testing is designed to detect errors in the ballot design or counting logic. It provides little or no benefit against deliberate attacks.

64. Much as Volkswagen's emission systems were designed to detect that they were being tested by the EPA and to only cheat while not under test, malware that has infected an optical scanner or BMD can be programmed to detect and circumvent L&A testing. For example, malware can be programmed to check the machine's clock and cheat only in the middle of election day, so that testing performed at an earlier or later time would show nothing amiss. Malware can also be programmed to cheat only after hundreds of ballots have been cast, so that more limited testing would not detect the fraud.

65. **Parallel testing.** I understand that Georgia has in the past employed a testing technique known as "parallel testing", and that the state might use this technique in the future to check whether BMDs correctly print voters' choices. In BMD parallel testing, poll workers periodically print test ballots during the election and confirm that the printouts match their selections.

66. Parallel testing cannot reliably determine that a BMD is working correctly. An attacker could program the BMD to modify the voter's selections on only certain printouts, and the selection could depend on a very large number of variables, including the time of day, the number of ballots cast, the voter's ballot selections, and whether the voter used options such as a large font size or an audio ballot. It is impossible for any practical amount of testing to examine all sets of conditions under which attackers might choose to cheat.[38]

67. In any event, investigation that occurs during the election is no help if the attacker's intention is to sabotage the voting process, such as by disabling the BMDs entirely. I am aware that Georgia's contingency plans call for having voters mark ballots by hand if BMDs are unavailable. However, an attacker might cause all BMDs to fail simultaneously over a large geographic area. To my knowledge, the state does not maintain sufficient quantities of pre-printed ballots to allow voting to continue under such a circumstance.

68. **Post-election audits.** Officials could potentially detect certain kinds of attacks by conducting a rigorous post-election audit of the paper ballots. For an audit to reliably detect vote-changing attacks, several requirements must be met. Among

[38] Philip B. Stark, "There is no Reliable Way to Detect Hacked Ballot-Marking Devices" (2019), https://www.stat.berkeley.edu/~stark/Preprints/bmd-p19.pdf.

them are: (i) the paper ballots being audited must correctly reflect voters' selections, (ii) the audit needs to be conducted manually, by having people inspect the ballots; (iii) the auditors need to inspect sufficiently many ballots to ensure that the probability that outcome-changing fraud could go undetected is low. In general, the closer the election result, the more ballots need to be audited in order to rule out fraud. Audits that limit the risk that outcome changing fraud will go undetected to no more than a pre-defined limit are called "risk-limiting audits" (RLAs).[39]

69. I understand that Georgia statute requires a state-wide post-election audit to be conducted no later than the November 2020 election.[40] However, that audit is not required to be risk-limiting. As a result, if there are close races in which an attacker changes the outcome by hacking the election equipment, there is a high probability that the audit would fail to uncover the attack.

70. Although some Georgia counties recently conducted small-scale audit pilots using risk-limiting techniques,[41] these audits achieved a low risk-limit only in

[39] Mark Lindeman and Philip B. Stark, "A Gentle Introduction to Risk-limiting Audits," in *IEEE Security and Privacy* (2012), https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.
[40] *See* O.C.G.A. § 21-2-498(b).
[41] Georgia Secretary of State's Office, "Risk-Limiting Audit Concludes Paper-Ballot System Accurate," (https://sos.ga.gov/index.php/elections/risk-limiting_audit_concludes_paper-ballot_system_accurate (last visited Feb. 17, 2020).

specific local races. An attacker could choose to target any race in any election, and an attack would likely not be detected in an RLA if it occurred in a race for which the RLA had a high effective risk-limit. To my knowledge, the Georgia Secretary of State has not announced plans to perform an RLA of *any* state-wide race.

71. No matter what auditing procedures Georgia applies, the state's widespread use of BMDs makes it possible for an attacker to undermine the integrity of the paper trail. Malware could cause the BMDs to print fraudulent selections, both in the barcode and the human-readable text. Such an attack would be impossible to detect by auditing the ballots, even with an RLA, because all records of the voter's intent would be wrong.

BMDs Create Additional Risks

72. The ICX BMDs are computers, they run outdated and vulnerable software, and they must be programmed using the State's election management system before every election. Attackers could potentially infect Georgia's BMDs with malware in several ways, including by spreading it from the election management system (EMS).

73. An attacker who infected the BMDs with malware could change the printed ballots. On a fraction of the ballots, the attacker could cause the human-readable text, the barcode, or both to reflect fraudulent choices rather than the voter's

selections. I will discuss two kinds of such misprinting attacks: attacks that change only the barcode and attacks that change both the barcode and the text.

74. **Misprinting only the barcode.** One kind of misprinting attack is a barcode-only attack. In this attack, malware would change a fraction of the BMD printouts so that they correctly showed the voter's selections in the human-readable text but encoded a different, fraudulent set of selections in the barcode.

75. If an attacker changes only the barcode, it would be impossible for voters to detect the fraud. Voters cannot read the barcodes, so there is no practical way for them to verify that the barcodes match their intended selections. Moreover, when scanning BMD ballots, the optical scanners count only the votes encoded in the barcodes and ignore the text entirely. This means that voters cannot verify the portion of their ballots that gets counted.

76. Officials could potentially detect a mismatch between the barcodes and the ballot text using a sufficiently rigorous post-election audit. However, to my knowledge, Georgia has not announced plans to perform any kind of audit that would compare the barcodes and the printed text, nor what specific measures would be taken to render any potential audit sufficiently comprehensive and reliable.

77. **Misprinting both the barcode and the text.** Malware could also cause the BMDs to print fraudulent selections in *both* the barcode and the human-readable

text. This attack would be impossible to detect by auditing the ballots, even with an RLA, because all records of the voter's intent would be wrong. Pre-election testing and parallel testing also cannot reliably detect such cheating. The only practical way to discover the attack would be if enough voters reviewed their ballots, noticed the errors, and alerted election officials.

78. Even if some voters did notice that their ballots were misprinted, the voters would have no way to prove that the BMDs were at fault. From an election official's perspective, the voters who reported problems might be mistaken or lying. Many voters would need to report that the BMDs misprinted their ballots before officials could be sure there was a systemic problem. Even then, there are no protocols or policies in Georgia that I have found that address how many voter complaints or other conditions involving BMDs would be required to support a finding—or even a robust investigation—of a systemic problem.

79. If officials did suspect that the BMDs had been attacked, there would be no straightforward way to respond or recover. The only recourse might be to rerun the election, which could be statewide involving millions of voters across Georgia.

80. **Voter verification provides insufficient protection.** Research shows that most voters do not review their BMD printouts, and that voters will likely fail

to detect a large majority of errors caused by a BMD attack. This means that a BMD paper trail is not a reliable record of the votes expressed by the voters.

81. In one study, researchers observed voters in two polling places during an election in Sevier County, Tennessee, which uses BMDs similar to Georgia's.[42] Nearly half of voters did not review the BMD printout *at all*, and those who did review it spent an average of only 4 seconds doing so. This suggests that voters are likely to detect at most about half of misprinted ballots, and possibly far fewer.

82. A second study, conducted by my research group at the University of Michigan, measured the rate at which voters detected errors during a realistic simulated election.[43] The voters used BMDs that my research assistants and I hacked so that one selection on each printout was wrong. We recorded how many participants reviewed their ballots and how many noticed the error and reported it to a poll worker. The study was peer reviewed and published at the IEEE Symposium on Security and Privacy in January 2020.

---

[42] Richard DeMillo, Robert Kadel, and Marilyn Marks, "What Voters are Asked to Verify Affects Ballot Verification: A Quantitative Analysis of Voters' Memories of Their Ballots" (Nov. 23, 2018), https://ssrn.com/abstract=3292208.

[43] Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman, "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?" in *Proceedings of the 41st IEEE Symposium on Security and Privacy* (2020), https://jhalderm.com/pub/papers/bmd-verifiability-sp20.pdf.

83. In the first part of the study, subjects were not prompted to review their ballots in any way. Under that condition, 60% of voters failed to review their ballots, and voters only reported 6.6% of errors. Considering only prominent "top of the ticket" races, voters reported only 14% of errors. These results imply that for every voter who notices that their ballot is misprinted and corrects it, there will likely be many more voters who fail to notice and have their votes stolen by the attacker.

84. In the second part of the study, we tested procedural changes to see whether they improved verification. Signage instructing voters to verify their ballots (as required in Georgia) did not increase error reporting. Other changes did help, but only to a limited extent. For example, when a poll worker verbally prompted the voter to review the ballot after it was printed, voters reported 15% of errors. In my opinion, it is unlikely that any purely procedural changes can enhance voters' error detection rates sufficiently to stop outcome-changing fraud in close elections when BMDs are used by all in-person voters.

85. My coauthors and I provide a mathematical model for estimating how many voters will report problems if BMDs are attacked in a way that changes an election outcome. The model illustrates how weak a defense voter verification provides when all in-person voters use BMDs.

86. Suppose there is a close election with an apparent margin of victory of 1% in favor of candidate A. If there had been no cheating, the result would have been a one-vote victory for candidate B, but an attacker hacked the BMDs so that they misprinted a small fraction of the ballots. If voters report 14% of misprinted ballots (the rate my study found for top-of-the-ticket contests), then only about 1 in 1200 BMD voters will report a problem—roughly one per precinct—even though the election outcome is wrong due to fraud. This is likely far too few complaints to alert officials or the public that there was a major, outcome-determinative problem.

87. Election officials are unlikely to take disruptive actions, like a protracted and expensive forensic investigation or ordering a new election, unless a much larger fraction of BMD voters report problems. Suppose officials would launch an investigation if more than 1% of BMD voters reported a problem. Under the scenario above, this condition would only be met if voters verified their ballots so carefully that they reported 67% of errors. This is ten times greater than the rate of error reporting my group observed in our study.

Georgia's Voting System was Vulnerable to Cyberattacks in 2018

88. Plaintiffs have asked me to opine on the security of Georgia's election system as it was used in 2018. From 2002 until the end of 2019, Georgia's primary polling place voting equipment was Diebold AccuVote TS and TSX direct-recording

electronic (DRE) voting machines. Georgia's DREs were "paperless," in that they did not create any kind of voter-verifiable paper record of individual votes. There is a broad scientific consensus that paperless DREs do not provide adequate security against cyberattacks.[44] Moreover, Georgia's DREs and election management systems used outdated software with widely documented vulnerabilities. In my opinion, Georgia's paperless DRE system was highly susceptible to cyberattacks that could change votes, erase votes, or cast extra votes.

89. The AccuVote TS and TSX are probably the most well-studied by security researchers of any voting machines in the world. Over the past 17 years, I, and other experts have repeatedly documented serious security problems with these machines and their election management system, as part of peer-reviewed and state-sponsored research studies. The vulnerabilities that affected Georgia's DRE system include numerous hardware and software security flaws, as well as architectural weaknesses. In tests, I have demonstrated that, in just a few seconds, anyone can install vote-stealing malware on these machines that will alter all records of every vote.[45]

---

[44] National Academies of Sciences, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy* (2018), http://nap.edu/25120.

[45] Ariel J. Feldman, J. Alex Halderman & Edward W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine*, Princeton University (2006), http://usenix.org/events/evt07/tech/full_papers/feldman/feldman.pdf.

90. In a 2006 study, collaborators and I demonstrated the vulnerabilities of the AccuVote TS by developing malware that could infect the machines and steal votes. The malware we created modifies all the vote records, audit logs, and protective counters stored by the machine, so that even careful forensic examination of the files would find nothing amiss. The malware was programmed to inspect each ballot as it was cast and modify the minimum number of votes necessary to ensure that the attacker's favored candidate always had at least a certain percentage of the vote total.

91. We also developed a voting machine virus that could spread the vote-stealing malware automatically from machine to machine during normal pre- and post-election activities. The virus propagated via the removable memory cards that election workers use to program the ballot design before every election and to offload election results. By exploiting vulnerabilities in the AccuVote software, an infected memory card can spread the voting machine virus to the machine. Once installed, the virus can copy itself to every memory card inserted into the infected machine. If those cards are inserted into other machines, they too will become infected.

92. In 2007, the Secretary of State of California organized a comprehensive election security examination, the California Top-to-Bottom Review (TTBR[46]), which examined systems including the AccuVote TSX. I was part of a team of six experts who spent approximately 30 days examining the source code to the AccuVote system. Also in 2007, the Secretary of State of Ohio conducted a similar security study and source code review (Project EVEREST[47]), which also covered the AccuVote TSX system.

93. Both studies found additional, extremely serious security vulnerabilities. The TTBR report documents 24 serious security issues in the AccuVote TSX. These include software flaws, including buffer-overflow vulnerabilities, that attackers could exploit to install malicious software on the voting machines and on the election management back-end systems used to design and tabulate ballots. These flaws could be exploited to spread a vote-stealing virus that would propagate even more efficiently and be more difficult to detect than the virus developed in my 2006 study.

---

[46] California Secretary of State, *Top-to-Bottom Review of Electronic Voting Systems* (2007), https://www.sos.ca.gov/elections/ovsta/frequently-requested-information/top-bottom-review/.

[47] Ohio Secretary of State, *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing* (Dec. 7, 2007), http://www.patrickmcdaniel.org/pubs/everest.pdf.

94. The software that performed election functions on the AccuVote TS and TSX is called BallotStation. I understand that the machines used in Georgia used BallotStation version 4.5.2, which was developed in 2005, and that Georgia did not ever update the BallotStation software to a newer version, even though newer versions were available. This software predates the California and Ohio studies, which examined version 4.6 in 2007. In my opinion, the serious vulnerabilities discovered in these studies almost certainly remained uncorrected in the software used on Georgia's voting machines through the end of 2019.

95. The election management system that was used with the AccuVote DREs is called the Global Election Management Environment ("GEMS"). Vulnerabilities in GEMS and BallotStation make it possible for an attacker who infiltrates a GEMS installation or its data files to spread vote-stealing malware to all voting machines that are programmed from that installation.

96. I understand that, for the November 2018 election, Georgia programmed its DREs as follows. Individuals working as third-party contractors for the Secretary of State prepared the initial ballot programming files for every Georgia county. To do so, they used copies of GEMS installed on computers in their homes, outside the physically secured environment of the Secretary of State's office. Once an initial version of the programming for a county had been completed, it was copied

to a USB drive and delivered to Michael Barnes, Director of the Center for Election Systems, at the Secretary of State's office. Barnes used his Internet-connected computer to inspect the files. He then transferred them into the State's central GEMS server environment on another USB drive.[48]

97. As a consequence of this workflow, ballot programming files for every county passed through an Internet-connected computer. In my opinion, attackers could have exploited this weakness to spread malware to the GEMS servers, and, ultimately, to DREs across the state.

98. I understand that, after workers at the SOS office finalized the ballot programming files, they delivered them to each county on a CD. Each county maintained its own GEMS server, to which workers copied files from the CD. Workers then used the county GEMS server to prepare memory cards for each DRE within the county.

99. In my opinion, an attacker who infiltrated the SOS GEMS system could have spread malware to the county GEMS servers by infecting the CDs used to distribute the files. Similarly, an attacker who infiltrated a county GEMS system

[48] Order at 28-31, *Curling v. Raffensperger*, No. 1:17-cv-2989-AT (N.D. Ga. Aug. 15, 2019), ECF No. 579.

could have spread vote-stealing malware to all DREs in the county by infecting the memory cards.

100. I am familiar with several countermeasures that the Georgia election system employed in 2018. These include parallel testing, logic and accuracy testing, anti-virus and end-point protection, tamper-evident seals, and network isolation of GEMS servers from the Internet. In my opinion, Georgia's election security countermeasures were inadequate to stop a sophisticated attacker, such as a hostile nation state, from infiltrating the election system, spreading malware to voting machines, and altering election outcomes.

101. In principle, it might be possible to detect whether Georgia's election system was infiltrated by attackers by conducting detailed digital forensics of the election equipment. As far as I can tell, *nobody* has ever performed a forensic examination of even a single Georgia DRE or GEMS server.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct, and that this declaration was executed this 18th day of February, 2020 in Philadelphia, Pennsylvania.

_____

J. ALEX HALDERMAN

EXHIBIT A

J. Alex Halderman

Professor, Computer Science and Engineering
University of Michigan

2260 Hayward Street
Ann Arbor, MI 48109 USA
(office) +1 734 647 1806
jhalderm@eecs.umich.edu

J.AlexHalderman.com

February 17, 2020

Research Overview

My research focuses on computer security and privacy, with an emphasis on problems that broadly impact society and public policy. Topics that interest me include software security, network security, data privacy, anonymity, surveillance, election cybersecurity, censorship resistance, computer forensics, ethics, and cybercrime. I'm also interested in the interaction of technology with politics and international affairs.

Selected Projects

'19: Leading Michigan Election Security Taskforce
'18: Commercial launch of Censys, Inc.
'17: Testimony to U.S. Senate Russia investigation
'17: Weaknesses in TLS interception middleboxes
'16: U.S. presidential election recounts
'16: Let's Encrypt HTTPS certificate authority
'16: DROWN: Attacking TLS with SSLv2
'15: Weak Diffie-Hellman and the Logjam attack
'14: Understanding Heartbleed's aftermath
'14: Security problems in full-body scanners
'14: Analysis of Estonia's Internet voting system
'13: ZMap Internet-wide network scanner
'12: Widespread weak keys in network devices
'11: Anticensorship in the network infrastructure
'10: Hacking Washington D.C.'s Internet voting
'10: Vulnerabilities in India's e-voting machines
'10: Reshaping developers' security incentives
'09: Analysis of China's Green Dam censorware
'09: Fingerprinting paper with desktop scanners
'08: Cold-boot attacks on encryption keys
'07: California's "top-to-bottom" e-voting review
'07: Machine-assisted election auditing
'06: The Sony rootkit: DRM's harmful side effects
'03: Analysis of MediaMax "shift key" DRM

Positions

- University of Michigan, Ann Arbor, MI
  Department of Electrical Engineering and Computer Science,
  Computer Science and Engineering Division

  Professor ... (2016–present)
  Associate Professor ... (2015–2016)
  Assistant Professor ... (2009–2015)

  Director, Center for Computer Security and Society (2014–present)
- Censys; Co-founder and Chief Scientist (2017–present)
- ISRG; Co-founder and Board Member (2013–present)

Education

- Ph.D. in Computer Science, Princeton University, June 2009
  Advisor: Ed Felten Committee: Andrew Appel, Adam Finkelstein, Brian Kernighan, Avi Rubin
  Thesis: *Investigating Security Failures and their Causes: An Analytic Approach to Computer Security*
- A.B. in Computer Science, *summa cum laude*, Princeton University, June 2003

Honors and Awards

- President's Award for National and State Leadership, University of Michigan (2020)
- Andrew Carnegie Fellowship (2019)
- Merit Network's Eric Aupperle Innovation Award (2017)
  ("named for Merit's first president, recognizes individuals that enhance their work by using networking and related technologies in exciting ways")
- Pwnie Award in the category of "Best Cryptographic Attack"
  for "DROWN: Breaking TLS using SSLv2," Black Hat 2016
- Finalist for 2016 Facebook Internet Defense Prize
  for "DROWN: Breaking TLS using SSLv2"
- Named one of Popular Science's "Brilliant 10" (2015) ("each year *Popular Science* honors the brightest young minds reshaping science, engineering, and the world")
- **Best Paper Award** of the 22nd ACM Conference on Computer and Communications Security
  for "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice" (2015)
- Pwnie Award in the category of "Most Innovative Research"
  for "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice," Black Hat 2015
- IRTF Applied Networking Research Prize for "Neither Snow Nor Rain Nor MITM... An Empirical Analysis of Email Delivery Security" (2015)
- Alfred P. Sloan Research Fellowship (2015)
- University of Michigan College of Engineering 1938 E Award (2015) ("recognizes an outstanding teacher in both elementary and advanced courses, an understanding counselor of students who seek guidance in their choice of a career, a contributor to the educational growth of the College, and a teacher whose scholarly integrity pervades his/her service and the profession of Engineering")
- Morris Wellman Faculty Development Assistant Professorship (2015)
  ("awarded to a junior faculty member to recognize outstanding contributions to teaching and research")
- **Best Paper Award** of the 14th ACM Internet Measurement Conference
  for "The Matter of Heartbleed" (2014)
- **Best Paper Award** of the 21st USENIX Security Symposium
  for "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices" (2012)
- Runner-up for 2012 PET Award for Outstanding Research in Privacy Enhancing Technologies
  for "Telex: Anticensorship in the Network Infrastructure" (2012)
- John Gideon Memorial Award from the Election Verification Network
  for contributions to election verification (2011)
- **Best Student Paper** of the 17th USENIX Security Symposium
  for "Lest We Remember: Cold Boot Attacks on Encryption Keys" (2008)
- Pwnie Award in the category of "Most Innovative Research"
  for "Lest We Remember: Cold Boot Attacks on Encryption Keys," Black Hat 2008

- Charlotte Elizabeth Procter Honorific Fellowship, Princeton University (2007)
  ("awarded in recognition of outstanding performance and professional promise, and represents high commendation from the Graduate School")
- National Science Foundation Graduate Research Fellowship (2004–2007)
- **Best Paper Award** of the 8th International Conference on 3D Web Technology for "Early Experiences with a 3D Model Search Engine" (2003)
- Princeton Computer Science Department Senior Award (2003)
- Accenture Prize in Computer Science, Princeton University (2002)
- Martin A. Dale Summer Award, Princeton University (2000)
- USA Computing Olympiad National Finalist (1996 and 1997)

Refereed Conference Publications

[1] **Can Voters Detect Malicious Manipulation of Ballot Marking Devices?**
Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. A. Halderman
To appear in *41st IEEE Symposium on Security and Privacy* ("Oakland"), May 2020.

[2] **Let's Encrypt: An Automated Certificate Authority to Encrypt the Entire Web**
Josh Aas, Richard Barnes, Benton Case, Zakir Durumeric, Peter Eckersley, Alan Flores-López, J. A. Halderman, Jacob Hoffman-Andrews, James Kasten, Eric Rescorla, Seth Schoen, and Brad Warren
26th ACM Conference on Computer and Communications Security (CCS), Nov. 2019.
Acceptance rate: 16%, 117/722.

[3] **Conjure: Summoning Proxies from Unused Address Space**
Sergey Frolov, Jack Wampler, Sze Chuen Tan, J. A. Halderman, Nikita Borisov, and Eric Wustrow
26th ACM Conference on Computer and Communications Security (CCS), Nov. 2019.
Acceptance rate: 16%, 117/722.

[4] **UnclearBallot: Automated Ballot Image Manipulation**
Matthew Bernhard, Kartikeya Kandula, Jeremy Wink, and J. A. Halderman
Proc. 4th International Joint Conference on Electronic Voting (E-Vote-ID), October 2019.
Acceptance rate: 29%, 13/45.

[5] **On the Usability of HTTPS Deployment**
Matthew Bernhard, Jonathan Sharman, Claudia Ziegler Acemyan, Philip Kortum, Dan S. Wallach, and J. A. Halderman
Proc. ACM Conference on Human Factors in Computing Systems (CHI), May 2019.
Acceptance rate: 24%, 705/2958.

[6] 403 Forbidden: A Global View of Geoblocking
Allison McDonald, Matthew Bernhard, Benjamin VanderSloot, Will Scott, J. A. Halderman, and Roya Ensafi
Proc. 18th ACM Internet Measurement Conference (IMC), October 2018.
Acceptance rate: 24%, 43/174.

[7] Quack: Scalable Remote Measurement of Application-Layer Censorship
Benjamin VanderSloot, Allison McDonald, Will Scott, J. A. Halderman, and Roya Ensafi
Proc. 27th USENIX Security Symposium, August 2018.
Acceptance rate: 19%, 100/524.

[8] Tracking Certificate Misissuance in the Wild
Deepak Kumar, Zhengping Wang, Matthew Hyder, Joseph Dickinson, Gabrielle Beck, David Adrian, Joshua Mason, Zakir Durumeric, J. A. Halderman, and Michael Bailey
Proc. 39th IEEE Symposium on Security and Privacy ("Oakland"), May 2018.
Acceptance rate: 11%, 63/549.

[9] Initial Measurements of the Cuban Street Network
Eduardo Pujol, Will Scott, Eric Wustrow, and J. A. Halderman
Proc. 17th ACM Internet Measurement Conference (IMC), London, November 2017.
Acceptance rate: 23%, 42/179.

[10] Public Evidence from Secret Ballots
Matthew Bernhard, Josh Benaloh, J. A. Halderman, Ronald L. Rivest, Peter Y. A. Ryan, Philip B. Stark, Vanessa Teague, Poorvi L. Vora, and Dan S. Wallach
Proc. 2nd International Joint Conference on Electronic Voting (E-Vote-ID), Bregenz, Austria, October 2017.

[11] Understanding the Mirai Botnet
Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. A. Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou
Proc. 26th USENIX Security Symposium, Vancouver, BC, August 2017.
Acceptance rate: 16%, 85/522.

[12] Security Challenges in an Increasingly Tangled Web
Deepak Kumar, Zane Ma, Zakir Durumeric, Ariana Mirian, Joshua Mason, J. A. Halderman, and Michael Bailey
Proc. 26th World Wide Web Conference (WWW), April 2017.
Acceptance rate: 17%, 164/966.

[13] The Security Impact of HTTPS Interception
Zakir Durumeric, Zane Ma, Drew Springall, Richard Barnes, Nick Sullivan, Elie Bursztein, Michael Bailey, J. A. Halderman, and Vern Paxson
Proc. 24th Network and Distributed Systems Symposium (NDSS), February 2017.
Acceptance rate: 16%, 68/423.

[14] Measuring Small Subgroup Attacks Against Diffie-Hellman
Luke Valenta, David Adrian, Antonio Sanso, Shaanan Cohney, Joshua Fried, Marcella Hastings, J. A. Halderman, and Nadia Heninger
Proc. 24th Network and Distributed Systems Symposium (NDSS), February 2017.
Acceptance rate: 16%, 68/423.

[15] An Internet-Wide View of ICS Devices
Ariana Mirian, Zane Ma, David Adrian, Matthew Tischer, Thasphon Chuenchujit, Tim Yardley, Robin Berthier, Josh Mason, Zakir Durumeric, J. A. Halderman, and Michael Bailey
Proc. 14th IEEE Conference on Privacy, Security, and Trust (PST), Auckland, NZ, December 2016.

[16] Implementing Attestable Kiosks
Matthew Bernhard, J. A. Halderman, and Gabe Stocco
Proc. 14th IEEE Conference on Privacy, Security, and Trust (PST), Auckland, NZ, December 2016.

[17] A Security Analysis of Police Computer Systems
Benjamin VanderSloot, Stuart Wheaton, and J. A. Halderman
Proc. 14th IEEE Conference on Privacy, Security, and Trust (PST), Auckland, NZ, December 2016.

[18] Measuring the Security Harm of TLS Crypto Shortcuts
Drew Springall, Zakir Durumeric, and J. A. Halderman
Proc. 16th ACM Internet Measurement Conference (IMC), Santa Monica, November 2016.
Acceptance rate: 25%, 46/184.

[19] Towards a Complete View of the Certificate Ecosystem
Benjamin VanderSloot, Johanna Amann, Matthew Bernhard, Zakir Durumeric, Michael Bailey, and J. A. Halderman
Proc. 16th ACM Internet Measurement Conference (IMC), Santa Monica, November 2016.
Acceptance rate: 25%, 46/184.

[20] DROWN: Breaking TLS using SSLv2
Nimrod Aviram, Sebastian Schinzel, Juraj Somorovsky, Nadia Heninger, Maik Dankel, Jens Steube, Luke Valenta, David Adrian, J. A. Halderman, Viktor Dukhovni, Emilia Käsper, Shaanan Cohney, Susanne Engels, Christof Paar, and Yuval Shavitt
Proc. 25th USENIX Security Symposium, Austin, TX, August 2016.
Acceptance rate: 16%, 72/463.
Tied for highest ranked submission.
Pwnie award for best cryptographic attack.
Facebook Internet Defense Prize finalist.

[21] FTP: The Forgotten Cloud
Drew Springall, Zakir Durumeric, and J. A. Halderman
Proc. 46th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Toulouse, June 2016.
Acceptance rate: 22%, 58/259.

[22] Android UI Deception Revisited: Attacks and Defenses
Earlence Fernandes, Qi Alfred Chen, Justin Paupore, Georg Essl, J. A. Halderman, Z. Morley Mao, and Atul Prakash
Proc. 20th International Conference on Financial Cryptography and Data Security (FC), Barbados, February 2016.

[23] Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice
David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. A. Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann
Proc. 22nd ACM Conference on Computer and Communications Security (CCS), Denver, CO, October 2015.
Acceptance rate: 19%, 128/659.
Best paper award. Perfect review score.
Pwnie award for most innovative research.
CACM Research Highlight.

[24] Censys: A Search Engine Backed by Internet-Wide Scanning
Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey, and J. A. Halderman
Proc. 22nd ACM Conference on Computer and Communications Security (CCS), Denver, CO, October 2015.
Acceptance rate: 19%, 128/659.

[25] Neither Snow Nor Rain Nor MITM...An Empirical Analysis of Email Delivery Security
Zakir Durumeric, David Adrian, Ariana Mirian, James Kasten, Elie Bursztein, Nicholas Lidzborski, Kurt Thomas, Vijay Eranti, Michael Bailey, and J. A. Halderman
Proc. 15th ACM Internet Measurement Conference (IMC), Tokyo, October 2015.
Acceptance rate: 26%, 44/169.
IRTF Applied Networking Research Prize winner.

[26] The New South Wales iVote System:
Security Failures and Verification Flaws in a Live Online Election
J. A. Halderman and Vanessa Teague
Proc. 5th International Conference on E-Voting and Identity (VoteID), Bern, Switzerland, September 2015.

[27] The Matter of Heartbleed
Zakir Durumeric, Frank Li, James Kasten, Johanna Amann, Jethro Beekman, Mathias Payer, Nicolas Weaver, David Adrian, Vern Paxson, Michael Bailey, and J. A. Halderman
Proc. 14th ACM Internet Measurement Conference (IMC), November 2014.
Acceptance rate: 23%, 43/188
Best paper award.
Honorable mention for Best dataset award.

[28] **Security Analysis of the Estonian Internet Voting System**
Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. A. Halderman
Proc. 21st ACM Conference on Computer and Communications Security (CCS), Scottsdale, AZ, November 2014.
Acceptance rate: 19%, 114/585.
Highest ranked submission.

[29] **Efficiently Auditing Multi-Level Elections**
Joshua A. Kroll, Edward W. Felten, and J. A. Halderman
Proc. 6th International Conference on Electronic Voting (EVOTE), Lochau, Austria, October 2014.

[30] **Security Analysis of a Full-Body Scanner**
Keaton Mowery, Eric Wustrow, Tom Wypych, Corey Singleton, Chris Comfort, Eric Rescorla, Stephen Checkoway, J. A. Halderman, and Hovav Shacham
Proc. 23rd USENIX Security Symposium, San Diego, CA, August 2014.
Acceptance rate: 19%, 67/350.

[31] **TapDance: End-to-Middle Anticensorship without Flow Blocking**
Eric Wustrow, Colleen Swanson, and J. A. Halderman
Proc. 23rd USENIX Security Symposium, San Diego, CA, August 2014.
Acceptance rate: 19%, 67/350.

[32] **An Internet-Wide View of Internet-Wide Scanning**
Zakir Durumeric, Michael Bailey, and J. A. Halderman
Proc. 23rd USENIX Security Symposium, San Diego, CA, August 2014.
Acceptance rate: 19%, 67/350.

[33] **Elliptic Curve Cryptography in Practice**
Joppe W. Bos, J. A. Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, and Eric Wustrow
Proc. 18th Intl. Conference on Financial Cryptography and Data Security (FC), March 2014.
Acceptance rate: 22%, 31/138.

[34] **Outsmarting Proctors with Smartwatches: A Case Study on Wearable Computing Security**
Alex Migicovsky, Zakir Durumeric, Jeff Ringenberg, and J. A. Halderman
Proc. 18th Intl. Conference on Financial Cryptography and Data Security (FC), March 2014.
Acceptance rate: 22%, 31/138.

[35] **Analysis of the HTTPS Certificate Ecosystem**
Zakir Durumeric, James Kasten, Michael Bailey, and J. A. Halderman
Proc. 13th ACM Internet Measurement Conference (IMC), Barcelona, Spain, October 2013.
Acceptance rate: 24%, 42/178.

[36] ZMap: Fast Internet-Wide Scanning and its Security Applications
Zakir Durumeric, Eric Wustrow, and J. A. Halderman
Proc. 22nd USENIX Security Symposium, Washington, D.C., August 2013.
Acceptance rate: 16%, 45/277.

[37] CAge: Taming Certificate Authorities by Inferring Restricted Scopes
James Kasten, Eric Wustrow, and J. A. Halderman
Proc. 17th Intl. Conference on Financial Cryptography and Data Security (FC), April 2013.

[38] Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices
Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. A. Halderman
Proc. 21st USENIX Security Symposium, pages 205–220, Bellevue, WA, August 2012.
Acceptance rate: 19%, 43/222.
Best paper award.
Named one of *Computing Reviews'* Notable Computing Books and Articles of 2012.

[39] Attacking the Washington, D.C. Internet Voting System
Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. A. Halderman
In Angelos D. Keromytis, editor, *Financial Cryptography and Data Security (FC)*, volume 7397 of *Lecture Notes in Computer Science*, pages 114–128. Springer, 2012.
Acceptance rate: 26%, 23/88.
Election Verification Network John Gideon Memorial Award.

[40] Telex: Anticensorship in the Network Infrastructure
Eric Wustrow, Scott Wolchok, Ian Goldberg, and J. A. Halderman
Proc. 20th USENIX Security Symposium, pages 459–474, San Francisco, CA, August 2011.
Acceptance rate: 17%, 35/204.
Runner-up for 2012 PET Award for Outstanding Research in Privacy Enhancing Technologies.

[41] Internet Censorship in China: Where Does the Filtering Occur?
Xueyang Xu, Z. Morley Mao, and J. A. Halderman
In Neil Spring and George F. Riley, editors, *Passive and Active Measurement*, volume 6579 of *Lecture Notes in Computer Science*, pages 133–142. Springer, 2011.
Acceptance rate: 29%, 23/79.

[42] Absolute Pwnage: Security Risks of Remote Administration Tools
Jay Novak, Jonathan Stribley, Kenneth Meagher, and J. A. Halderman
In George Danezis, editor, *Financial Cryptography and Data Security (FC)*, volume 7035 of *Lecture Notes in Computer Science*, pages 77–84. Springer, 2011.
Acceptance rate: 20%, 15/74.

[43] Security Analysis of India's Electronic Voting Machines
Scott Wolchok, Eric Wustrow, J. A. Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp
Proc. 17th ACM Conference on Computer and Communications Security (CCS), pages 1–14. ACM, Chicago, IL, October 2010.

Acceptance rate: 17%, 55/320.
Highest ranked submission.

[44] Sketcha: A Captcha Based on Line Drawings of 3D Models
Steve Ross, J. A. Halderman, and Adam Finkelstein
Proc. 19th International World Wide Web Conference (WWW), pages 821–830. ACM, Raleigh, NC, April 2010.
Acceptance rate: 12%, 91/754.

[45] Defeating Vanish with Low-Cost Sybil Attacks Against Large DHTs
Scott Wolchok, Owen S. Hofmann, Nadia Heninger, Edward W. Felten, J. A. Halderman, Christopher J. Rossbach, Brent Waters, and Emmett Witchel
In *Proc. 17th Network and Distributed System Security Symposium (NDSS)*. Internet Society, San Diego, CA, February–March 2010.
Acceptance rate: 15%, 24/156.

[46] Fingerprinting Blank Paper Using Commodity Scanners
William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. A. Halderman, and Edward W. Felten
IEEE Symposium on Security and Privacy ("Oakland"), pages 301–314. IEEE, May 2009.
Acceptance rate: 10%, 26/254.

[47] Lest We Remember: Cold-Boot Attacks on Encryption Keys
J. A. Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten
Proc. 17th USENIX Security Symposium, pages 45–60, San Jose, CA, July 2008.
Acceptance rate: 16%, 27/170.
Best student paper award.
Pwnie award for most innovative research.
CACM Research Highlight.

[48] Harvesting Verifiable Challenges from Oblivious Online Sources
J. A. Halderman and Brent Waters
Proc. 14th ACM Conference on Computer and Communications Security (CCS), pages 330–341. ACM, Washington, D.C., October 2007.
Acceptance rate: 18%, 55/302.

[49] Lessons from the Sony CD DRM Episode
J. A. Halderman and Edward W. Felten
Proc. 15th USENIX Security Symposium, pages 77–92, Vancouver, BC, August 2006.
Acceptance rate: 12%, 22/179.

[50] A Convenient Method for Securely Managing Passwords
J. A. Halderman, Brent Waters, and Edward W. Felten
Proc. 14th International World Wide Web Conference (WWW), pages 471–479. ACM, Chiba, Japan, May 2005.
Acceptance rate: 14%, 77/550.

[51] New Client Puzzle Outsourcing Techniques for DoS Resistance
Brent Waters, Ari Juels, J. A. Halderman, and Edward W. Felten
Proc. 11th ACM Conference on Computer and Communications Security (CCS), pages 246–256. ACM, Washington, D.C., October 2004.
Acceptance rate: 14%, 35/251.

[52] Early Experiences with a 3D Model Search Engine
Patrick Min, J. A. Halderman, Michael Kazhdan, and Thomas Funkhouser
Proc. 8th International Conference on 3D Web Technology (Web3D), pages 7–18. ACM, Saint Malo, France, March 2003.
Best paper award.

Book Chapters

[53] Practical Attacks on Real-world E-voting
J. A. Halderman
In Feng Hao and Peter Y. A. Ryan (Eds.), *Real-World Electronic Voting: Design, Analysis and Deployment*, pages 145–171, CRC Press, December 2016.

Journal Publications

[54] Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice
David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. A. Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann
Communications of the ACM, 61(1):106–114, 2019.

[55] Lest We Remember: Cold-Boot Attacks on Encryption Keys
J. A. Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten
Communications of the ACM, 52(5):91–98, 2009.

[56] A Search Engine for 3D Models
Thomas Funkhouser, Patrick Min, Michael Kazhdan, Joyce Chen, J. A. Halderman, David P. Dobkin, and David Jacobs
ACM Transactions on Graphics (TOG), 22(1):83–105, 2003.

Refereed Workshop Publications

[57] Bernoulli Ballot-Polling: A Manifest Improvement for Risk-Limiting Audits
Kellie Ottoboni, Matthew Bernhard, J. A. Halderman, Ronald L. Rivest, and Philip B. Stark
Proc. 4th Workshop on Advances in Secure Electronic Voting, Feb. 2019.

[58] An ISP-Scale Deployment of TapDance
Sergey Frolov, Fred Douglas, Will Scott, Allison McDonald, Benjamin VanderSloot, Rod Hynes, Adam Kruger, Michalis Kallitsis, David G. Robinson, Nikita Borisov, J. A. Halderman, and Eric Wustrow
Proc. 7th USENIX Workshop on Free and Open Communications on the Internet (FOCI), Aug. 2017.

[59] Content-Based Security for the Web
Alexander Afanasyev, J. A. Halderman, Scott Ruoti, Kent Seamons, Yingdi Yu, Daniel Zappala, and Lixia Zhang
Proc. 2016 New Security Paradigms Workshop (NSPW), September 2016.

[60] Umbra: Embedded Web Security through Application-Layer Firewalls
Travis Finkenauer and J. A. Halderman
Proc. 1st Workshop on the Security of Cyberphysical Systems (WOS-CPS), Vienna, Austria, September 2015.

[61] Replication Prohibited: Attacking Restricted Keyways with 3D Printing
Ben Burgess, Eric Wustrow, and J. A. Halderman
Proc. 9th USENIX Workshop on Offensive Technologies (WOOT), Washington, DC, August 2015.

[62] Green Lights Forever: Analyzing the Security of Traffic Infrastructure
Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J. A. Halderman
Proc. 8th USENIX Workshop on Offensive Technologies (WOOT), San Diego, CA, August 2014.

[63] Zippier ZMap: Internet-Wide Scanning at 10Gbps
David Adrian, Zakir Durumeric, Gulshan Singh, and J. A. Halderman
Proc. 8th USENIX Workshop on Offensive Technologies (WOOT), San Diego, CA, August 2014.

[64] Internet Censorship in Iran: A First Look
Simurgh Aryan, Homa Aryan, and J. A. Halderman
Proc. 3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI), Washington, D.C., August 2013.

[65] Illuminating the Security Issues Surrounding Lights-Out Server Management
Anthony Bonkoski, Russ Bielawski, and J. A. Halderman
Proc. 7th USENIX Workshop on Offensive Technologies (WOOT), Washington, D.C., August 2013.

[66] Crawling BitTorrent DHTs for Fun and Profit
Scott Wolchok and J. A. Halderman
Proc. 4th USENIX Workshop on Offensive Technologies (WOOT), Washington, D.C., August 2010.

[67] Can DREs Provide Long-Lasting Security?
The Case of Return-Oriented Programming and the AVC Advantage
Steve Checkoway, Ariel J. Feldman, Brian Kantor, J. A. Halderman, Edward W. Felten, and Hovav Shacham
Proc. 2009 USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop / Workshop on Trustworthy Elections (EVT/WOTE), Montreal, QC, August 2009.

[68] You Go to Elections with the Voting System You Have:
Stop-Gap Mitigations for Deployed Voting Systems
J. A. Halderman, Eric Rescorla, Hovav Shacham, and David Wagner
In *Proc. 2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT)*, July 2008.

[69] In Defense of Pseudorandom Sample Selection
Joseph A. Calandrino, J. A. Halderman, and Edward W. Felten
Proc. 2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT), San Jose, CA, July 2008.

[70] Security Analysis of the Diebold AccuVote-TS Voting Machine
Ariel J. Feldman, J. A. Halderman, and Edward W. Felten
Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT), Washington, D.C., August 2007.

[71] Machine-Assisted Election Auditing
Joseph A. Calandrino, J. A. Halderman, and Edward W. Felten
Proc. USENIX/ACCURATE Electronic Voting Technology Workshop (EVT), Washington, D.C., August 2007.

[72] Privacy Management for Portable Recording Devices
J. A. Halderman, Brent Waters, and Edward W. Felten
Proc. 2004 ACM Workshop on Privacy in the Electronic Society (WPES), pages 16–24, ACM, Washington, D.C., October 2004.
Acceptance rate: 22%, 10/45.

[73] Evaluating New Copy-Prevention Techniques for Audio CDs
J. A. Halderman
In Joan Feigenbaum, editor, *Digital Rights Management*, volume 2696 of *Lecture Notes in Computer Science*, pages 101–117. Springer, 2003.

Selected Other Publications

[74] U.S. House Testimony Regarding Federal Funding for Election Cybersecurity
J. A. Halderman
Testimony before the U.S. House Appropriations Subcommittee on Financial Service and General Government, "Election Security: Ensuring the Integrity of U.S. Election Systems", February 27, 2019.

[75] I Hacked an Election. So Can the Russians.
J. A. Halderman
Video op/ed in collaboration with *The New York Times*, April 5, 2018.

[76] U.S. Senate Testimony Regarding Russian Interference in the 2016 U.S. Elections
J. A. Halderman
Testimony before the U.S. Senate Select Committee on Intelligence, June 21, 2017.

[77] Here's How to Keep Russian Hackers from Attacking the 2018 Elections
J. A. Halderman and J. Talbot-Zorn
The Washington Post, June 21, 2017.

[78] Want to Know if the Election was Hacked? Look at the Ballots
J. A. Halderman
Posted on Medium, November 23, 2016. (Read by over a million people.)

[79] The Security Challenges of Online Voting Have Not Gone Away
Robert Cunningham, Matthew Bernhard, and J. A. Halderman
IEEE Spectrum, November 3, 2016.

[80] TIVOS: Trusted Visual I/O Paths for Android
Earlence Fernandes, Qi Alfred Chen, Georg Essl, J. A. Halderman, Z. Morley Mao, and Atul Prakash
Technical report, Computer Science and Engineering Division, University of Michigan, Ann Arbor, MI, May 2014.

[81] Tales from the Crypto Community:
The NSA Hurt Cybersecurity. Now It Should Come Clean
Nadia Heninger and J. A. Halderman
Foreign Affairs, October 23, 2013.

[82] Ethical Issues in E-Voting Security Analysis
David G. Robinson and J. A. Halderman
In George Danezis, Sven Dietrich, and Kazue Sako, editors, *Financial Cryptography and Data Security*, volume 7126 of *Lecture Notes in Computer Science*, pages 119–130. Springer, 2011.
Invited paper.

[83] To Strengthen Security, Change Developers' Incentives
J. A. Halderman
IEEE Security & Privacy, 8(2):79–82, March/April 2010.

[84] Analysis of the Green Dam Censorware System
Scott Wolchok, Randy Yao, and J. A. Halderman
Technical report, Computer Science and Engineering Division, University of Michigan, Ann Arbor, MI, June 2009.

[85] AVC Advantage: Hardware Functional Specifications
J. A. Halderman and Ariel J. Feldman
Technical report, TR-816-08, Princeton University Computer Science Department, Princeton, New Jersey, March 2008.

[86] Source Code Review of the Diebold Voting System
J. A. Calandrino, A. J. Feldman, J. A. Halderman, D. Wagner, H. Yu, and W. Zeller
Technical report, California Secretary of State's "Top-to-Bottom" Voting Systems Review (TTBR), July 2007.

[87] Digital Rights Management, Spyware, and Security
Edward W. Felten and J. A. Halderman
IEEE Security & Privacy, 4(1):18–23, January/February 2006.

[88] Analysis of the MediaMax CD3 Copy-Prevention System
J. A. Halderman
Technical report, TR-679-03, Princeton University Computer Science Department, Princeton, New Jersey, October 2003.

Selected Legal and Regulatory Filings

[89] Request for DMCA Exemption: Security Research
Petition to the U.S. Copyright Office of Ed Felten and J. Alex Halderman, represented by Elizabeth Field, Justin Manusov, Brett Hildebrand, Alex Kimata, and Blake Reid, regarding the Seventh Triennial Section 1201 Proceeding, 2017–18.
(*Outcome:* Requested exemption granted in part.)

[90] Request for DMCA Exemption: Security Research
Petition to the Librarian of Congress of S. M. Bellovin, M. Blaze, E. W. Felten, J. A. Halderman, and N. Heninger, represented by Andrea Matwyshyn, regarding the U.S. Copyright Office 2014–2015 DMCA Anticircumvention Rulemaking, Nov. 2014.
(*Outcome:* Requested exemption granted in part.)

[91] Request for DMCA Exemption: Games with Insecure DRM and Insecure DRM Generally
Petition to the Librarian of Congress of J. A. Halderman, represented by B. Reid, P. Ohm, H. Surden, and J. B. Bernthal, regarding the U.S. Copyright Office 2008–2010 DMCA Anticircumvention Rulemaking, Dec. 2008.
(*Outcome:* Requested exemption granted in part.)

[92] Request for DMCA Exemption for Audio CDs with Insecure DRM
Petition to the Librarian of Congress of E. Felten and J. A. Halderman, represented by D. Mulligan and A. Perzanowski, regarding the U.S. Copyright Office 2005–2006 DMCA Anticircumvention Rulemaking, Dec. 2005.
(*Outcome:* Requested exemption granted in part.)

Patents

[93] Controlling Download and Playback of Media Content
Wai Fun Lee, Marius P. Schilder, Jason D. Waddle, and J. A. Halderman
U.S. Patent No. 8,074,083, issued Dec. 2011.

[94] System and Method for Machine-Assisted Election Auditing
Edward W. Felten, Joseph A. Calandrino, and J. A. Halderman
U.S. Patent No. 8,033,463, issued Oct. 2011.

Speaking

Major Invited Talks and Keynotes

- U.S. House Testimony Regarding Federal Funding for Election Cybersecurity
  Testimony before the U.S. House Appropriations Subcommittee on Financial Service and General Government, Feburary 27, 2019.
- Election Cybersecurity Progress Report: Will the U.S. be Ready for 2020?
  35c3, Leipzig, December 27, 2018.
- Cyberattacks on Election Infrastructure
  Keynote speaker, DIMVA 2018, Paris, June 29, 2018.
- U.S. Senate Testimony Regarding Russian Interference in the 2016 U.S. Elections
  Testimony before the U.S. Senate Select Committee on Intelligence, June 21, 2017.
- Recount 2016: A Security Audit of the U.S. Presidential Election
  Keynote talk, NDSS 2017, February 27, 2017.
- Recount 2016: An Uninvited Security Audit of the U.S. Presidential Election
  33c3, Hamburg, December 28, 2016.
- Elections and Cybersecurity: What Could Go Wrong?
  Keynote speaker, Merit Security Summit, Ypsilanti, MI, November 7, 2016.
- Let's Encrypt
  Invited speaker, TTI/Vanguard conference on Cybersecurity, Washington, D.C., Sept. 28, 2016.
- Elections and Cybersecurity: What Could Go Wrong?
  Keynote speaker, 19th Information Security Conference (ISC), Honolulu, September 9, 2016.
- Internet Voting: What Could Go Wrong?
  Invited speaker, USENIX Enigma, San Francisco, January 27, 2016.
- Logjam: Diffie-Hellman, Discrete Logs, the NSA, and You
  32c3, Hamburg, December 29, 2015.
- The Network Inside Out: New Vantage Points for Internet Security
  Invited talk, China Internet Security Conference (ISC), Beijing, September 30, 2015.
- The Network Inside Out: New Vantage Points for Internet Security
  Keynote speaker, ESCAR USA (Embedded Security in Cars), Ypsilanti, Michigan, May 27, 2015.
- Security Analysis of the Estonian Internet Voting System
  31c3, Hamburg, December 28, 2014.
- The Network Inside Out: New Vantage Points for Internet Security
  Keynote speaker, 14th Brazilian Symposium on Information Security and Computer Systems (SBSeg), Belo Horizonte, Brazil, November 4, 2014.

- **Empirical Cryptography: Measuring How Crypto is Used and Misused Online**
  Keynote speaker, 3rd International Conference on Cryptography and Information Security in Latin America (Latincrypt), Florianópolis, Brazil, September 2014.
- **Healing Heartbleed: Vulnerability Mitigation with Internet-wide Scanning**
  Keynote speaker, 11th Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), London, July 10, 2014.
- **Fast Internet-wide Scanning and its Security Applications**
  30c3, Hamburg, December 28, 2013.
- **Challenging Security Assumptions.** Three-part tutorial. 2nd TCE Summer School on Computer Security, Technion (Haifa, Israel), July 23, 2013.
- **Verifiably Insecure: Perils and Prospects of Electronic Voting**
  Invited talk, Computer Aided Verification (CAV) 2012 (Berkeley, CA), July 13, 2012.
- **Deport on Arrival: Adventures in Technology, Politics, and Power**
  Invited talk, 20th USENIX Security Symposium (San Francisco, CA), Aug. 11, 2011.
- **Electronic Voting: Danger and Opportunity**
  Keynote speaker, ShmooCon 2008 (Washington, D.C.), Feb. 15, 2008.

Selected Talks (2009–present)

- **Let's Encrypt: An Automated Certificate Authority to Encrypt the Entire Web**
  Invited speaker, OWASP Copenhagen, November 25, 2019.
- **Cybersecurity and U.S. Elections**
  Invited speaker, CyberSec & AI Prague, October 25, 2019; Invited speaker, Indiana University Research, February 7, 2019; Invited speaker, Arizona State, January 16, 2019; Invited speaker, University of San Diego, November 16, 2018; Invited speaker, UMass Amherst, October 31, 2018; Invited speaker, U-M Alumni Association, October 18, 2018; Invited speaker, MIT EmTech, August 13, 2018; Invited speaker, DEFCON Voting Village, August 10, 2018; Invited speaker, U.S. Irvine Election Security Summit, Irvine, March 13, 2018; Invited speaker, Global Election Summit, San Francisco, May 17, 2017; Invited speaker, Wolverine Caucus Forum, Lansing, February 21, 2017; Invited speaker, CSE Science on Screen at Michigan Theater, Ann Arbor, January 25, 2017.
- **Congressional Briefing on Election Cybersecurity.**
  Hosted by Rep. Mike Quigley and Rep. John Katko; September 26, 2018.
- **Congressional Briefing on Election Cybersecurity.**
  Co-panelists: Harri Hursti, Tony Schaffer, Liz Howard, Shantiel Soeder, Dan Savickas; moderator: Trey Greyson. July 10, 2018.
- **Congressional Briefing: Hacked Voting Machine Demonstration.**
  Hosted by Senator Kamala Harris and Senator James Lankford. April 12, 2018.
- **Congressional Briefing: Strengthening Election Cybersecurity.**
  Co-panelists: Nicole Austin-Hillery, Tony Shaffer, Bruce Fein, Susan Greenhalgh, Shane Schoeller. October 19, 2017.

- **The Security Impact of HTTPS Interception.** Invited talk, GOTO Copenhagen, Oct. 2, 2017.
- **Congressional Briefing: Free, Automated, and Open Web Encryption.** August 8, 2017; hosted by Congressional Cybersecurity Caucus.
- **Let's Encrypt: A Certificate Authority to Encrypt the Entire Web.** Invited talk, Summer school on real-world crypto and privacy, Croatia, June 9, 2017; Invited talk, Cubaconf, Havana, April 25, 2016.
- **Congressional Briefing: Strengthening Election Cybersecurity.** Co-panelists: James Woolsey, Tony Shaffer, Lawrence Norden, Susan Greenhalgh, James Scott; moderator: Karen Greenberg. May 15, 2017.
- **The Legacy of Export-grade Cryptography in the 21st Century.** Invited talk, Summer school on real-world crypto and privacy, Croatia, June 9, 2016.
- **Logjam: Diffie-Hellman, Discrete Logs, the NSA, and You.** Invited talk, NYU Tandon School of Engineering, April 8, 2016 [host: Damon McCoy]; Invited talk, UIUC Science of Security seminar, February 9, 2016 [host: Michael Bailey].
- **The Network Inside Out: New Vantage Points for Internet Security.** Invited talk, Qatar Computing Research Institute, Doha, May 24, 2015; Invited talk, University of Chile, Santiago, April 8, 2015; Invited talk, Princeton University, October 15, 2014; Invited talk, U.T. Austin, March 9, 2014.
- **Decoy Routing: Internet Freedom in the Network's Core.** Invited speaker, Internet Freedom Technology Showcase: The Future of Human Rights Online, New York, Sep. 26, 2015.
- **The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election.** 5th International Conference on E-Voting and Identity (VoteID), Bern, Switzerland, Sep. 3, 2015; Invited talk, IT Univ. of Copenhagen, Sep. 1, 2015; Invited talk (with Vanessa Teague), USENIX Journal of Election Technologies and Systems Workshop (JETS), Washington, D.C., Aug. 11, 2015.
- **Security Analysis of the Estonian Internet Voting System.** Invited talk, 5th International Conference on E-Voting and Identity (VoteID), Bern, Switzerland, Sep. 3, 2015; Invited talk, Google, Mountain View, CA, June 3, 2014; Invited talk, Copenhagen University, June 12, 2014.
- **Indiscreet Tweets.** Rump session talk; 24th USENIX Security Symposium, Washington, D.C., August 12, 2015.
- **How Diffie-Hellman Fails in Practice.** Invited talk, IT Univ. of Copenhagen, May 22, 2015.
- **Influence on Democracy of Computers, Internet, and Social Media.** Invited speaker, Osher Lifelong Learning Institute at the University of Michigan, March 26, 2015.
- **E-Voting: Danger and Opportunity.** Invited talk, University of Chile, Santiago, April 7, 2015; Keynote speaker, 14th Brazilian Symposium on Information Security and Computer Systems (SBSeg), Belo Horizonte, Brazil, November 3, 2014; Crypto seminar, University of Tartu, Estonia, October 10, 2013; Invited speaker, US–Egypt Cyber Security Workshop, Cairo, May 28, 2013; Invited speaker, First DemTech Workshop on Voting Technology for Egypt, Copenhagen, May 1, 2013; Invited keynote, 8th CyberWatch Mid-Atlantic CCDC, Baltimore, MD, Apr. 10, 2013;

Invited speaker, Verifiable Voting Schemes Workshop, University of Luxembourg, Mar. 21, 2013; Invited speaker, MHacks hackathon, Ann Arbor, MI, Feb. 2, 2013; Public lecture, U. Michigan, Nov. 6, 2012.

- Internet Censorship in Iran: A First Look. 3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI), Aug. 13, 2013.
- Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices. Invited talk, NSA, Aug. 8, 2013; Invited talk, Taiwan Information Security Center Workshop, National Chung-Hsing University (Taichung, Taiwan), Nov. 16, .2012
- Securing Digital Democracy. U. Maryland, Apr. 8, 2013 [host: Jonathan Katz]; CMU, Apr. 1, 2013 [host: Virgil Gligor]; Cornell, Feb. 28, 2013 [host: Andrew Myers].
- Telex: Anticensorship in the Network Infrastructure. Invited speaker, Academia Sinica (Taipei), Nov. 14, 2012 [host: Bo-Yin Yang]; TRUST Seminar, U.C., Berkeley, Dec. 1, 2011 [host: Galina Schwartz]; Think Conference, Nov. 5, 2011; Ideas Lunch, Information Society Project at Yale Law School, Oct. 26, 2011; Invited speaker, Committee to Protect Journalists Online Press Freedom Summit (San Francisco), Sept. 27, 2011.
- Deport on Arrival: Adventures in Technology, Politics, and Power. Guest lecture, U-M School of Art and Design, Nov 5, 2012 [host: Osman Khan]; Invited speaker, CS4HS Workshop, U. Michigan, Aug. 21, 2012; Invited speaker, U. Michigan IEEE, Feb. 15, 2012.
- Attacking the Washington, D.C. Internet Voting System. Invited speaker, International Foundation for Election Systems (IFES), Nov. 2, 2012 [host: Michael Yard]; Invited speaker, IT University of Copenhagen, May 11, 2012 [host: Carsten Schürmann].
- Voter I*Don't*. Rump session talk; 21st USENIX Security Symposium (Bellevue, WA), Aug. 8, 2012; Rump session talk; EVT/WOTE '12 (Bellevue, WA), Aug. 6, 2012 [with Josh Benaloh].
- Reed Smith's Evening with a Hacker. Keynote speaker (New Brunswick, NJ), Oct. 20, 2011.
- Are DREs Toxic Waste? Rump session talk, 20th USENIX Security Symposium (San Francisco), Aug. 10, 2011; Rump session talk, EVT/WOTE '11 (San Francisco), Aug. 8, 2011.
- Security Problems in India's Electronic Voting Machines. Dagstuhl seminar on Verifiable Elections and the Public (Wadern, Germany), July 12, 2011; Harvard University, Center for Research on Computation and Society (CRCS) seminar, Jan. 24, 2011 [host: Ariel Procaccia]; U. Michigan, CSE seminar, Nov. 18, 2010 [with Hari Prasad]; MIT, CSAIL CIS Seminar, Nov. 12, 2010 [with Hari Prasad; host: Ron Rivest]; Distinguished lecture, U.C. San Diego, Department of Computer Science, Nov. 9, 2010 [with Hari Prasad; host: Hovav Shacham]; U.C. Berkeley, Center for Information Technology Research in the Interest of Society (CITRIS), Nov. 8, 2010 [with Hari Prasad; host: Eric Brewer]; Google, Inc., Tech Talk (Mountain View, CA), Nov. 5, 2010 [with Hari Prasad; host: Marius Schilder]; U.C., Berkeley TRUST Security Seminar, Nov. 4, 2010 [with Hari Prasad; host: Shankar Sastry]; Stanford University, CS Department, Nov. 3, 2010 [with Hari Prasad; host: David Dill]; Princeton University, Center for Information Technology Policy, Oct. 28, 2010 [with Hari Prasad, host: Ed Felten]; University of Texas at Austin, Department of Computer Science, Aug. 27, 2010 [host: Brent Waters].

- **Ethical Issues in E-Voting Security Analysis.** Invited talk, Workshop on Ethics in Computer Security Research (WECSR) (Castries, St. Lucia), Mar. 4, 2011 [with David Robinson].
- **Electronic Voting: Danger and Opportunity.** Invited speaker, "Interfaces 10: Technology, Society and Innovation," Center for Technology and Society (CTS/FGV) (Rio de Janeiro), Dec. 2, 2010 [host: Ronaldo Lemos]; Invited speaker, Conference on "EVMs: How Trustworthy?," Centre for National Renaissance (Chennai, India), Feb. 13, 2010; Google, Inc., Tech Talk (Mountain View, CA), Jan. 10, 2008; Star Camp (Cape Town, South Africa), Dec. 8, 2007; Lehigh University, Nov. 27, 2007; Princeton OiT Lunch-'n-Learn, Oct. 24, 2007; University of Waterloo (Canada), Feb. 28, 2007.
- **A New Approach to Censorship Resistance.** Think Conference, Nov. 7, 2010.
- **Practical AVC-Edge CompactFlash Modifications can Amuse Nerds [PACMAN].** Rump session, 19th USENIX Security Symposium (Washington, D.C.), Aug. 11, 2010; Rump session, EVT/WOTE '10 (Washington, D.C.), Aug. 9, 2010.
- **Legal Challenges to Security Research.** Guest lecture, Law 633: Copyright, U. Michigan Law School, Apr. 7, 2010; Invited talk, University of Florida Law School, Oct. 12, 2006.
- **Adventures in Computer Security.** Invited talk, Greenhills School, grades 6–12 (Ann Arbor, MI), Mar. 8, 2010.
- **The Role of Designers' Incentives in Computer Security Failures.** STIET Seminar, U. Michigan, Oct. 8, 2009.
- **Cold-Boot Attacks Against Disk Encryption.** Invited speaker, SUMIT 09 Security Symposium, U. Michigan, Oct. 20, 2009.
- **On the Attack.** Distinguished lecture, U.C. Berkeley EECS, Nov. 18, 2009.

Selected Other Speaking (2010–present)

- Panelist: **How Adversaries Can Erode Public Trust in Democratic Institutions.** Co-panelists: Hany Farid, Ron Rivest, Suzanne Spaulding; moderator: James E. Boasberg. D.C. Circuit Judicial Conference, Cambridge, Maryland, June 26, 2019.
- **Alumni-Faculty Forum: Cold War 2.0: Russia, Cybersecurity and Hacking.** Co-panelists: Walter Slocombe, Alexander Southwell, Ishani Sud; moderator: Jonathan Mayer. June 1, 2018.
- Panelist: **"Critical Infrastructure" Designation for Election Operations: Risks, Mitigations, & Import for 2018.** Election Verification Network Conference, Miami, March 16, 2018.
- Panelist: **The Technology of Voting: Risks & Opportunities.** U.C. Irvine Cybersecurity and Policy Research Institute, March 13, 2018.
- Panelist: **Election Law Conflicts and the Vulnerability of our Election Systems.** Co-panelists: Stephen Berzon, Holly Lake, Harvey Saferstein. Ninth Circuit Judicial Conference, July 18, 2017.
- Moderator: **Apple & the FBI: Encryption, Security, and Civil Liberties.** Panelists: Nate Cardozo and Barbara McQuade. U-M Dissonance Speaker Series, April 12, 2016.

- Moderator: Privacy, IT Security and Politics. Panelists: Ari Schwartz and David Sobel. U-M ITS SUMIT_2015, Oct. 22, 2015.
- Panelist: The Future of E-Voting Research. 5th International Conference on E-Voting and Identity (VoteID), Bern, Switzerland, Sep. 4, 2015.
- Moderator: Panel on Research Ethics. 24th USENIX Security Symposium, Washington, D.C., August 13, 2015.
- Panelist: Theories of Privacy in Light of "Big Data." Michigan Telecommunications and Technology Law Review Symposium on Privacy, Technology, and the Law, University of Michigan Law School, Feb. 21, 2015.
- Panelist: Measuring Privacy. Big Privacy symposium, Princeton University CITP, Apr. 26, 2013 [moderator: Ed Felten].
- Panelist: Civil Society's Challenge in Preserving Civic Participation. The Public Voice workshop: Privacy Rights are a Global Challenge, held in conjunction with the 34th International Conference of Data Protection and Privacy Commissioners, Punta del Este, Uruguay, Oct. 22, 2012 [moderator: Lillie Coney].
- Panelist: Election Technologies: Today and Tomorrow. Microsoft Faculty Summit (Redmond), July 17, 2012 [moderator: Josh Benaloh].
- Panelist: Is America Ready to Vote on the Internet? CSPRI Seminar, George Washington University (Washington, D.C.), May 16, 2012 [moderator: Lance Hoffman].
- Panelist: Technical Methods of Circumventing Censorship. Global Censorship Conference, Yale Law School, Mar. 31, 2012.
- Panelist: Internet Voting. RSA Conference (San Francisco), Mar. 1, 2012 [moderator: Ron Rivest].
- Panelist: The Law and Science of Trustworthy Elections. Association of American Law Schools (AALS) Annual Meeting, Jan. 5, 2012 [moderator: Ron Rivest].
- Panelist: Connecticut Secretary of State's Online Voting Symposium (New Britain, CT), Oct. 27, 2011 [moderator: John Dankosky].
- Panelist: Cyber Security / Election Technology. Overseas Voting Foundation Summit, Feb. 10, 2011 [moderator: Candice Hoke].
- ~~Tutorial speaker/organizer: Security Issues in Electronic Voting, ICISS (Gandhinagar, India), Dec. 15, 2010~~ [canceled under threat of deportation].
- Invited testimony: On D.C. Board of Elections and Ethics Readiness for the Nov. 2010 General Election. D.C. Council Hearing, Oct. 8, 2010.
- Panelist and organizer: India's Electronic Voting Machines. EVT/WOTE (Washington, D.C.), Aug. 9, 2010.
- Panelist: Ethics in Networking and Security Research. ISOC Network and Distributed System Security Symposium (San Diego, CA), Mar. 2, 2010 [moderator: Michael Bailey].

Advising and Mentoring

Graduate Students

- Allison McDonald (Ph.D. in progress; Facebook Emerging Scholar Fellowship)
- Matthew Bernhard (Ph.D. in progress)
- Benjamin VanderSloot (Ph.D. in progress)
- David Adrian (Ph.D. 2019; went on to principal engineer at Censys)
- Andrew Springall (Ph.D. 2018; went on to tenure-track faculty position at Auburn)
- Zakir Durumeric (Ph.D. 2017; Google Ph.D. Fellowship in Computer Security; went on to tenure-track faculty position at Stanford)
- Eric Wustrow (Ph.D. 2016; went on to tenure-track faculty position at U. Colorado, Boulder)
- James Kasten (Ph.D. 2015; went on to software engineering position at Google)
- Rose Howell (M.S. 2018)
- Travis Finkenauer (M.S. 2016; went on to security position at Juniper Networks)
- Scott Wolchok (M.S. 2011; went on to software engineering position at Facebook)

Post Docs

- Will Scott (2017–18)
- Colleen Swanson (2014–15)

Doctoral Committees

- Arunkumaar Ganesan (C.S. Ph.D. expected 2019)
- David Adrian (C.S. Ph.D. 2019, Michigan; chair)
- Andrew Springall (C.S. Ph.D. 2018, Michigan; chair)
- Kyong Tak Cho (C.S. Ph.D. 2018, Michigan)
- Armin Sarabi (E.E. Ph.D. 2018, Michigan)
- Zakir Durumeric (C.S. Ph.D. 2017, Michigan; chair)
- Armin Sarabi (E.E. Ph.D. 2017, Michigan)
- Eric Crockett (C.S. Ph.D 2017, Georgia Tech)
- Kassem Fawaz (C.S. Ph.D. 2017, Michigan)
- Amir Rahmati (C.S. Ph.D. 2017, Michigan)
- Earlence Fernandez (C.S. Ph.D. 2017, Michigan)
- Huan Feng (C.S. Ph.D. 2016, Michigan)
- Jakub Czyz (C.S. Ph.D. 2016, Michigan)
- Denis Bueno (C.S. Ph.D. 2016, Michigan)
- Eric Wustrow (C.S. Ph.D. 2016, Michigan; chair)
- James Kasten (C.S. Ph.D. 2015, Michigan; chair)
- Jing Zhang (C.S. Ph.D. 2015, Michigan)
- Katharine Cheng (C.S. Ph.D. 2012, Michigan)

- Matt Knysz (C.S. Ph.D. 2012, Michigan)
- Zhiyun Qian (C.S. Ph.D. 2012, Michigan)
- Xin Hu (C.S. Ph.D. 2011, Michigan)
- Ellick Chan (C.S. Ph.D. 2011, UIUC)

Undergraduate Independent Work

- 2019: Scott Bays, Kevin Chang, Jensen Hwa, Nicholas Matton, Henry Meng, Ellen Tsao, Hassaan Ali Watoo
- 2018: Jensen Hwa, Henry Meng, Armando Ruvalcaba
- 2017: Gabrielle Beck, Alex Holland
- 2016: Ben Burgess, Noah Duchan, Mayank Patke
- 2015: Ben Burgess, Rose Howell, Vikas Kumar, Ariana Mirian, Zhi Qian Seah
- 2014: Christopher Jeakle, Andrew Modell, Kollin Purcell
- 2013: David Adrian, Anthony Bonkoski, Alex Migicovsky, Andrew Modell, Jennifer O'Neil
- 2011: Yilun Cui, Alexander Motalleb
- 2010: Arun Ganesan, Neha Gupta, Kenneth Meagher, Jay Novak, Dhritiman Sagar, Samantha Schumacher, Jonathan Stribley
- 2009: Mark Griffin, Randy Yao

Teaching

- **Introduction to Computer Security**, EECS 388, University of Michigan
  Terms: Winter 2020, Fall 2019, Winter 2019, Winter 2017, Fall 2016, Fall 2015, Fall 2014, Fall 2013, Fall 2011, Fall 2010, Fall 2009
  Created new undergrad security elective that has grown to reach >750 students/year. An accessible intro, teaches the security mindset and practical skills for building and analyzing security-critical systems.
- **Surveillance Law and Technology** (with Margo Schlanger), EECS 598-007 / LAW 441-1, University of Michigan, Fall 2019.
- **Election Cybersecurity**, EECS 498, University of Michigan, Fall 2018.
- **Computer and Network Security**, EECS 588, University of Michigan
  Terms: Winter 2016, Winter 2015, Winter 2014, Winter 2013, Winter 2012, Winter 2011, Winter 2010, Winter 2009
  Redesigned core grad-level security course. Based around discussing classic and current research papers and performing novel independent work. Provides an intro. to systems research for many students.
- **Securing Digital Democracy**, Coursera (MOOC)
  Designed and taught a massive, open online course that explored the security risks—and future potential—of electronic voting and Internet voting technologies; over 20,000 enrolled students.

Professional Service

Program Committees

- 2019 ACM Internet Measurement Conference (IMC '19)
- 2017 ACM Conference on Computer and Communications Security (CCS '17)
- 2017 ISOC Network and Distributed Systems Security Symposium (NDSS '17)
- 2016 ACM Internet Measurement Conference (IMC '16)
- 2016 USENIX Security Symposium (Sec '16)
- 2016 International Joint Conference on Electronic Voting (E-VOTE-ID '16)
- 2016 Workshop on Advances in Secure Electronic Voting (Voting '16)
- 2015 ACM Conference on Computer and Communications Security (CCS '15)
- 2015 ACM Internet Measurement Conference (IMC '15)
- 2015 USENIX Security Symposium (Sec '15)
- 2014 ACM Conference on Computer and Communications Security (CCS '14)
- 2014 USENIX Security Symposium (Sec '14)
- 2013 ACM Conference on Computer and Communications Security (CCS '13)
- **Program co-chair,** 2012 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE '12)
- 2012 Workshop on Free and Open Communications on the Internet (FOCI '12)
- 2012 IEEE Symposium on Security and Privacy ("Oakland" '12)
- 2012 International Conference on Financial Cryptography and Data Security (FC '12)
- 2011 Workshop on Free and Open Communications on the Internet (FOCI '11)
- 2011 Electronic Voting Technology Workshop (EVT/WOTE '11)
- 2010 ACM Conference on Computer and Communications Security (CCS '10)
- 2010 USENIX/ACCURATE/IAVOSS Electronic Voting Technology Workshop (EVT '10)
- 2010 USENIX Security Symposium (Sec '10)
- 2010 IEEE Symposium on Security and Privacy (Oakland '10)
- 2010 International World Wide Web Conference (WWW '10)
- 2009 ACM Conference on Computer and Communications Security (CCS '09)
- 2009 ACM Workshop on Digital Rights Management (DRM '09)
- 2009 ACM Workshop on Multimedia Security (MMS '09)
- 2009 USENIX Workshop on Offensive Technologies (WOOT '09)
- 2009 International World Wide Web Conference (WWW '09)
- 2008 ACM Conference on Computer and Communications Security (CCS '08)
- 2008 ACM Workshop on Privacy in the Electronic Society (WPES '08)
- 2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '08)
- 2008 International World Wide Web Conference (WWW '08)

Boards

- Board of Directors of Internet Security Research Group (2014–present)
- Board of Advisors for the Verified Voting Foundation (2012–present)
- External Advisory Board for the DemTech Project, IT University of Copenhagen (2011–2016)
- Advisory Council for the Princeton University Department of Computer Science (2012–2014)

Government Service

- Michigan Secretary of State's Election Security Advisory Commission (co-chair, 2019–)

Department and University Service

- Lab Director, CSE Systems Lab (2018–present)
- CSE Hiring Committee (member, 2018–present)
- Faculty Advisor for Michigan Hackers student group (2012–present)
- CSE Graduate Affairs Committee (member, 2014–2017)
- CSE Undergraduate Program Advising (CS/ENG) (2011–2017)
- Faculty Senate, Rules Committee of the Senate Assembly (member, 2011–12)
- CSE Graduate Admissions Committee (member, 2010–11)
- CSE Graduate Committee (member, 2009–10)

CERTIFICATE OF SERVICE

I hereby certify that, on February 18, 2020, I caused to be served the foregoing **REPORT OF PLAINTIFFS' EXPERT WITNESS J. ALEX HALDERMAN** by filing it through the Court's ECF system, which will serve the following counsel:

Chris Carr, Esq.
Attorney General
Dennis Dunn, Esq.
Deputy Attorney General
Russell Willard, Esq.
Senior Assistant Attorney General
Georgia Office of the Attorney General
40 Capitol Square
Atlanta, GA 30334
ccarr@law.ga.gov
ddunn@law.ga.gov
rwillard@law.ga.gov

Joshua Barrett Belinfante, Esq.
Vincent Robert Russo, Jr., Esq.
Brian Edward Lake, Esq.
Carey Allen Miller, Esq.
Alexander Denton, Esq.
Special Assistant Attorneys General
Robbins Ross Alloy Belinfante Littlefield, LLC
500 Fourteenth St., N.W.
Atlanta, GA 30318
Telephone: (678) 701-9381
Fax: (404) 856-3250
jbelinfante@robbinsfirm.com
blake@robbinsfirm.com
vrusso@robbinsfirm.com
cmiller@robbinsfirm.com
adenton@robbinsfirm.com

Bryan P. Tyson, Esq.
Bryan F. Jacoutot, Esq.
Diana LaRoss, Esq.
Special Assistant Attorneys General
Taylor English Duma LLP
1600 Parkwood Circle
Suite 200
Atlanta, GA 30339
Telephone: (678) 336-7249
btyson@taylorenglish.com
bjacoutout@taylorenglish.com
dlaross@taylorenglish.com

/s/ Leslie J. Bryan
Leslie J. Bryan
Georgia Bar No. 091175

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FAIR FIGHT ACTION, INC, *et al.*,
Plaintiffs,
v.
BRAD RAFFENSPERGER, *et al.*,
Defendants.

Civ. Act. No. 18-cv-5391 (SCJ)

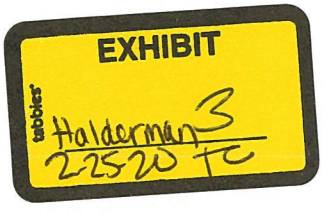
SUPPLEMENT TO THE EXPERT REPORT OF J. ALEX HALDERMAN

Plaintiffs hereby supplement the Expert Report of J. Alex Halderman by supplying signature pages. When Dr. Halderman sent the final report to counsel, he inadvertently omitted the signature pages. Those pages are attached hereto.

This, the19th day of February, 2020.

/s/ Leslie J. Bryan

Allegra J. Lawrence (GA Bar No. 439797)
Leslie J. Bryan (GA Bar No. 091175)
Maia Cogen (GA Bar No. 832438)
Suzanne Smith Williams (GA Bar No. 526105)
LAWRENCE & BUNDY LLC
1180 West Peachtree Street
Suite 1650
Atlanta, GA 30309
Telephone: (404) 400-3350
Fax: (404) 609-2504
allegra.lawrence-hardy@lawrencebundy.com
leslie.bryan@lawrencebundy.com
maia.cogen@lawrencebundy.com
suzanne.williams@lawrencebundy.com



Thomas R. Bundy (Admitted *pro hac vice*)
LAWRENCE & BUNDY LLC
8115 Maple Lawn Boulevard
Suite 350
Fulton, MD 20789
Telephone: (240) 786-4998
Fax: (240) 786-4501
thomas.bundy@lawrencebundy.com

Dara Lindenbaum (Admitted *pro hac vice*)
SANDLER REIFF LAMB ROSENSTEIN & BIRKENSTOCK, P.C.
1090 Vermont Avenue, NW
Suite 750
Washington, DC 20005
Telephone: (202) 479-1111
Fax: 202-479-1115
lindenbaum@sandlerreiff.com

Elizabeth Tanis (GA Bar No. 697415)
John Chandler (GA Bar No. 120600)
957 Springdale Road, NE
Atlanta, GA 30306
Telephone: (404) 771-2275
beth.tanis@gmail.com
jachandler@gmail.com

Kurt G. Kastorf (GA Bar No. 315315)
THE SUMMERVILLE FIRM, LLC
1226 Ponce de Leon Avenue, NE
Atlanta, GA 30306
Telephone: (770) 635-0030
Fax: (770) 635-0029
kurt@summervillefirm.com

Matthew G. Kaiser (Admitted *pro hac vice*)
Sarah R. Fink (Admitted *pro hac vice*)
Scott S. Bernstein (Admitted *pro hac vice*)
Norman G. Anderson (Admitted *pro hac vice*)
KAISERDILLON PLLC
1099 Fourteenth Street, NW
Eighth Floor West
Washington, DC 20005
Telephone: (202) 640-2850
Fax: (202) 280-1034
mkaiser@kaiserdillon.com
sfink@kaiserdillon.com
sbernstein@kaiserdillon.com
nanderson@kaiserdillion.com

Andrew D. Herman (Admitted *pro hac vice*)
Nina C. Gupta (Admitted *pro hac vice*)
MILLER & CHEVALIER CHARTERED
900 Sixteenth Street, NW
Washington, DC 20006
Telephone: (202) 626-5800
Fax: (202) 626-5801
aherman@milchev.com
ngupta@milchev.com

Kali Bracey (Admitted *pro hac vice*)
JENNER & BLOCK LLP
1099 New York Avenue, NW
Suite 900
Washington, DC 20001
Telephone: (202) 639-6000
Fax: (202) 639-6066
kbracey@jenner.com

Jeremy M. Creelan (Admitted *pro hac vice*)
Jeremy H. Ershow (Admitted *pro hac vice*)
JENNER & BLOCK LLP
919 Third Avenue
New York, New York 10022
Telephone: (212) 891-1600
Fax: (212) 891-1699
jcreelan@jenner.com
jershow@jenner.com

Von A. DuBose
DUBOSE MILLER LLC
75 14th Street N.E., Suite 2110
Atlanta, GA 30309
Telephone: (404) 720-8111
Fax: (404) 921-9557
dubose@dubosemiller.com

Johnathan Diaz (Admitted *pro hac vice*)
Paul M. Smith (Admitted *pro hac vice*)
CAMPAIGN LEGAL CENTER
1101 14 St. NW Suite 400
Washington, DC 20005
Telephone: (202)736-2200
psmith@campaignlegal.org
jdiaz@campaignlegal.org

Counsel for Fair Fight Action, Inc.; Care in Action, Inc.; Ebenezer Baptist Church of Atlanta, Georgia, Inc.; Baconton Missionary Baptist Church, Inc.; Virginia-Highland Church, Inc.; and The Sixth Episcopal District, Inc.

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FAIR FIGHT ACTION, et al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	Civ. Action No. 1:18-cv-05391-SCJ
	)	
BRAD RAFFENSPERGER, in his official capacity as Secretary of State of the State of Georgia, et al.,	)	
	)	
Defendants.	)	

EXPERT REPORT OF J. ALEX HALDERMAN

Professor of Computer Science & Engineering
Director, University of Michigan Center for Computer Security and Society
University of Michigan
Beyster Building, Room 4717
2260 Hayward Street
Ann Arbor, MI 48109-2121

When Dr. Halderman sent the final report to counsel, he inadvertently omitted the signature pages. Those pages are attached hereto.

February 18, 2020.

J. Alex Halderman, Ph.D.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct, and that this declaration was executed this 18th day of February, 2020 in Philadelphia, Pennsylvania.

J. ALEX HALDERMAN

CERTIFICATE OF SERVICE

I hereby certify that on this, the 19th day of February 2020, I electronically filed the foregoing **SUPPLEMENT TO THE EXPERT REPORT OF J. ALEX HALDERMAN** with the Clerk of Court using the CM/ECF system, which will automatically send notification of such filing to Counsel of Record:

Chris Carr, Esq.
Attorney General
Dennis Dunn, Esq.
Deputy Attorney General
Russell Willard, Esq.
Senior Assistant Attorneys General
Georgia Office of the Attorney General
40 Capitol Square
Atlanta, GA 30334
Telephone: (404) 656-3300
Fax: (404) 657-8733
ccarr@law.ga.gov
ddunn@law.ga.gov
rwillard@law.ga.gov

Bryan Tyson, Esq.
Bryan Jacoutot, Esq.
Diane F. LaRoss, Esq.
Taylor English Duma LLP
1600 Parkwood Circle
Suite 200
Atlanta, GA 30339
Telephone: (678) 336-7249
Fax: (404) 856-3250
btyson@taylorenglish.com
bjacoutot@taylorenglish.com
dlaross@taylorenglish.com

Joshua Barrett Belinfante, Esq.
Brian Edward Lake, Esq.
Carey Allen Miller, Esq.
Vincent Robert Russo, Jr., Esq.
Alexander Denton, Esq.
Robbins Ross Alloy Belinfante Littlefield, LLC -Atl
500 Fourteenth Street, NW
Atlanta, GA 30318
Telephone: (678) 701-9381
Fax: (404) 856-3250
jbelinfante@robbinsfirm.com
blake@robbinsfirm.com
cmiller@robbinsfirm.com
vrusso@robbinsfirm.com
adenton@robbinsfirm.com

/s/ Leslie J. Bryan
Leslie J. Bryan
Georgia Bar No. 091175

EVN 2019 – Moving the Needle: Securing and Auditing Our Elections

The Election Verification Network 2019 Annual Conference will be held **March 13-15 in Washington DC** at George Washington University.

Join us for a stimulating and timely conference that will also feature keynote speeches on the top election security issues. Attendance at EVN 2019 is by invitation. Please contact us for more information.

Session topics will include: Federal legislation on election security, election integrity litigation in the states, cyber infrastructure and election security, audit experiences- 2018, VVSG and standards, second generation election technology.

The conference will be held Thursday March 14 – Friday, March 15 8:30am to 5:30pm at the George Washington University School of Engineering and Applied Science, 800 22nd Street, NW, Washington, DC 20052 (Google Maps)

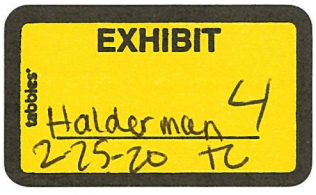
Welcome reception: Wednesday March 13 at 5pm at the Churchill Hotel Kalorama Room, 914 Connecticut Avenue NW, Washington DC (Google Maps).

Agenda

This program may be subject to change

Download the program agenda (Word)

List of attendees with bios (PDF)



The entire program will be live-streamed and recorded.

Join the live stream starting at 8:15am March 14

Wednesday, March 13

5pm – 7pm Welcome Reception (at the Churchill Hotel, open to all conference registrants)

Thursday, March 14

7:45am Check-in and Breakfast

8:15am Welcome and Introductions
Liz Howard, The Brennan Center for Justice
Poorvi Vora, George Washington University

8:30am Opening Remarks by U.S. Senator Ron Wyden, D-Oregon
Introduced by Greg Miller, Open Source Election Technology (OSET) Institute
Senator Wyden's biography *(PDF)*

9:00am Break

9:15am Remarks by David Sanger, National Security Correspondent, The New York Times and author of "The Perfect Weapon: War, Sabotage and Fear in the Cyber Age."
Introduced by Poorvi Vora, George Washington University
David Sanger's biography *(PDF)*

10:00am Break

10:15am Federal Legislation on Election Security
Election security continues to garner much attention in the 116th Congress. Staff for the lawmakers leading the way on federal election security reform will discuss the aims and options key lawmakers are weighing as they try to improve election security through federal legislation.

Moderator: Susan Greenhalgh, National Election Defense Coalition

Panelists: Jacob Barton, Senate Intelligence Committee (majority); Moira Bergen, House Homeland Security Committee (majority); Lindsey Kerr, Senate Rules Committee (minority)

11:30am Break

11:45am Election Integrity Litigation in the States

What's at stake nationally for election integrity in the litigation pending in Georgia and South Carolina, and why every EVNer will want to follow it closely.

Moderator: Candice Hoke, Cleveland-Marshall College of Law and Center for Cybersecurity & Privacy Protection

Panelists: Bruce Brown, Esq., Bruce P. Brown, Law, LLC; Max Feldman, Brennan Center for Justice; Larry Schwartztol, Protect Democracy

1:00pm Lunch

Announcement by Joe Kiniry and Dan Zimmerman, Galois and Free & Fair

1:45pm Usability and Voter Verification

Security often comes with a usability price. What are the issues arising from usability and accessibility that are pertinent to the ability of voters to verify their paper records?

Moderator: Matt Bernhard, University of Michigan, Ann Arbor

Panelists: Josh Benaloh, Microsoft Research; Michelle Bishop, National Disability Rights Network; J. Alex Halderman, University of Michigan, Ann Arbor

3:00pm Break

3:15pm Next Generation Voting Systems

This panel will discuss the current landscape of voting technology, discussing aspects of the security, accessibility, and usability of newer systems. The goal is to understand how recommendations made by the verifiable election community impact voting technology in practice, so we can better tailor our security and verifiability recommendations to make them more likely to be adopted and meaningfully deployed in practice.

Moderator: Matt Bernhard, University of Michigan, Ann Arbor

Panelists: Tina Barton, City of Rochester Hills, MI; Dana DeBeauvoir, Travis County, TX; Eddie Perez, Open Source Election Technology (OSET) Institute

4:30pm Break

4:45pm Annual EVN Awards

Chairperson: Susannah Goodman, Common Cause

Committee: Eddie Hailes, Advancement Project; Mark Lindeman, Verified Voting; Noel Runyan, Personal Data Systems; Poorvi Vora, George Washington University

Award descriptions

Previous award winners

2019 award winners

- Public Service for Improved Elections Award
  Neal Kelley
- John Gideon Memorial Election Advocacy Award
  Neal McBurnett
- Innovation Award
  Mayuri Sridhar and Kellie Ottoboni
- Election Integrity Research Excellence Award
  Rebecca Mercuri
- Journalism Award
  Eric Geller
- Full Tilt Advocacy Achievement Award
  Luther Weeks
- Long-Term Contributor Award
  Susan Dzieduszcka-Suinat

5:45pm Buffet Dinner

8:00pm Bus departs from George Washington University SEAS to The Churchill Hotel

Friday, March 15

8:15am Check-in and Continental Breakfast

8:45am Announcements

9:00am Opening Keynote – U.S. Congressman Jamie Raskin, Maryland 8th Congressional District

Election Vendor Security Act

Introduced by Senator William C. Smith, Jr., MD

Representative Raskin's biography *(PDF)*

9:45am Break

10:00am Keynote- Suzanne Spaulding, Senior Adviser for Homeland Security and Director of the Defending Democratic Institutions Project, International Security Program, Center for Strategic and International Studies (CSIS)

Introduced by Poorvi Vora, George Washington University

Suzanne Spaulding's biography *(PDF)*

10:30am Break

10:45am The Role of the Election Assistance Commission in Election Integrity

Moderator: Liz Howard, The Brennan Center for Justice

Panelists: EAC Commissioner Thomas Hicks; EAC Commissioner Benjamin Hovland; EAC Commissioner Donald Palmer

EAC slides

11:30am Break

11:45am VVSG Standards and Certification

This panel will discuss the Voluntary Voting Systems Guidelines (VVSG), Common Data Formats (CDF's), and other standards for election systems and data, as well as federal and state certification for standards compliance.

Moderator: John McCarthy, Verified Voting

Panelists: Joe Kiniry, Free & Fair and Galois; Sindhu Ramachandran, Pennsylvania Dept. of State; John Wack, NIST

12:45 pm Lunch

1:25pm Milestones in Post-Election Tabulation Audits

In the last year, several states broke new ground in post-election auditing — more than fit on one panel! We'll hear about risk-limiting audit pilots in Virginia, Michigan, and Rhode Island, plus Wisconsin's first-ever pre-certification audit. What was learned, and how can we build on the progress?

Moderator: Mark Lindeman, Verified Voting

Panelists: Brenda Cabrera, City of Fairfax, VA; Karen McKim, Wisconsin Election Integrity; Miguel Nunez, Rhode Island Board of Elections; Ronald L. Rivest, Massachusetts Institute of Technology (MIT)

Karen McKim's slides

2:25pm Break

2:35pm Voter Registration Databases and the Security of Voter Registration

US voter registration systems have been actively targeted by foreign adversaries in recent elections. This panel explores threats related to voter registration systems and defensive controls that can be used to strengthen VRDB security.

Moderator: Josh Franklin, Outstack Technologies

Panelists: Dr. Beata Martin-Rozumilowicz, International Foundation for Electoral Systems (IFES); John Dziurlaj, Turnout LLC

Josh Franklin's slides

John Dziurlaj's slides

Dr. Martin-Rozumilowicz' slides

3:35pm Break

3:45pm Partnerships and Progress

This panel will discuss the progress made in the effort to make our elections more secure and the various partnerships between election security experts and advocates, election officials and national security officials.

Moderator: Doug Kellner, New York State Board of Elections

Panelists: Monica Childers; Matt Masterson, U.S. Department of Homeland Security; Maurice Turner, Center for Democracy and Technology

5:00pm Close and toast

Eddie Hailes, Jr., Advancement Project

5:45pm Bus departs for The Churchill Near Embassy Row

Travel

The Churchill Hotel near Embassy Row is the official hotel of the 2019 EVN conference and will offer rooms to attendees at the conference rate of $199 plus tax **until** the room block is full or Friday **February 15**. Please follow this link: EVN DC- Web Link Churchill Hotel DC or call 800-424-2464 or 201-797-2000 ask for group reservations and request the EVN Conference rate.

The University is approximately 1 mile from the hotel. EVN will provide a bus once in the morning from the hotel to the conference and once in the afternoon from the conference to the hotel. Attendees also may secure their own transportation to and from the University.

This conference is sponsored in part by

Microsoft

verifiedvoting

Our Goal: A truly secure election system

OSET INSTITUTE

Search EVN

Enter Keywords

Email Us: info@electionverification.org

Just over a decade ago, a small group of election-related professionals concerned with the integrity and improvement of U.S. voting systems considered the potential of a gathering place for leaders, experts and policy makers...one where they could exchange information, collaborate on ideas, share challenges and solutions, and serve as a trusted advisory resource for those responsible for local, statewide, and national elections. Out of that concept, the Election Verification Network (EVN) was born. Our mission includes two interwoven goals: to support and maintain voting that is accessible, private, reliable, and secure; and elections that are transparent, accurate, and verifiable.

Who We Are & What We Do

Over time, we have grown to include over 200 participants, including computer scientists, election officials, voting activists, political scientists, attorneys, and others whose expertise reflects the many facets of contemporary voting. EVN involvement is invitation-only, and our participants are rigorously nonpartisan, working effectively together across disciplines and opinions, unraveling the complexities that a sometimes divisive and increasingly tech-enabled and tech-vulnerable world presents.

Participants | Jurisdictions | University Affiliations | **Organizations**

EVN participants are associated with a wide range of organizations*.

**These institutions do not directly participate in EVN, and no endorsement is implied.*

- Advancement Project
- Brennan Center for Justice at NYU School of Law
- California Voter Foundation
- Center for Voting Technology Research (VoTeR Center)
- Citizens' Alliance for Secure Elections, Ohio
- Citizens for Election Integrity Minnesota
- Coalition for Peace Action
- Coalition for Voting Integrity, Pennsylvania
- Coloradans for Voting Integrity
- Common Cause

- Common Cause New Mexico
- CTVotersCount
- E-Voter Education Project
- Elections By the People
- Electronic Frontier Foundation
- Florida Voters Foundation
- Galois
- Helios Voting
- Humboldt County Election Transparency Project
- Humphrey School of Public Affairs Program For Excellence in Election Administration
- International Foundation for Electoral Systems
- Lawyers' Committee for Civil Rights Under Law
- Mary Berryman Agard & Associates
- Microsoft Research
- National Coalition on Black Civic Participation
- National Conference of State Legislatures
- National Institute of Standards and Technology
- North Carolina Coalition for Verified Voting
- Open Source Digital Voting Foundation
- Overseas Vote Foundation
- Public Interest Pictures
- SAVE Our Votes: Secure, Accessible, Verifiable Elections for Maryland
- South Carolina Progressive Network
- Texas Safe Voting Coalition
- United Voters of New Mexico
- Usability in Civic Life
- Verified Voting Foundation
- VotePA
- Voter Action
- VotersUnite

Election Integrity

Election integrity is at the root of every conversation we have, every question we discuss, ev concern that an official or administrator brings to Ask Our Election Experts. We are working toward a future of maximum voter participation, unimpeded by practices or systems that de any voter or group of voters from exercising their right to weigh in on elections and issues.

> "I have not seen a more diverse, dedicated, passionate, nor capable group of people committed to protecting that mo basic right of democracy, the right of the people to vote."
>
> *Mark Earley,*
>
> Supervisor of Elections, Leon County Florida

Funding

The Election Verification Network is self-funded, largely from donations received during our annual "Twelve Days of Giving" campaign, which runs from "Giving Tuesday" to mid-December. Significant donors from the campaign are recognized through our "Champions of Giving" program.

(Donations are welcome at any time during the year.)

U.S. House Appropriations Subcommittee on Financial Service and General Government
"Election Security: Ensuring the Integrity of U.S. Election Systems"
February 27, 2019

Statement of Dr. J. Alex Halderman
Professor of Computer Science and Engineering, University of Michigan
Director, Michigan Center for Computer Security and Society

Chairman Quigley, Ranking Member Graves, and distinguished members, thank you for the opportunity to testify about this urgent matter of national security.

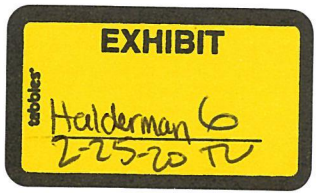
Three years ago, the United States Presidential election was attacked. Hackers penetrated political campaigns and leaked internal communications online, they manipulated social media in an effort order to sow discord, and they targeted our election infrastructure, including voter registration systems in at least 18 states. These attacks were about more than undermining voter confidence. In the assessment of the Director of National Intelligence, they marked a "significant escalation" of foreign "efforts to undermine the U.S.-led liberal democratic order".[1]

After two years of investigation by Congress and the intelligence community, we know that the attackers had the capability to do even more damage than they did. The Senate Select Committee on Intelligence has concluded that in some states, attackers "were in a position to, at a minimum, alter or delete voter registration data."[2] Had they done so (and had it gone undetected), there would have been widespread chaos on Election Day, as voters across the vulnerable states showed up to the polls only to be told they weren't registered. We were spared such a blow to the foundations of American democracy only because Russia chose not to pull the trigger.

Next time, things could be much worse, and it's not just voter registration systems that are at risk: the nation's voting machines are stunningly vulnerable to attacks that could sabotage the voting process or even invisibly alter tallies and change election outcomes. I know because I have developed such attacks myself as part of over a decade of research into election security threats and defenses.[3] Last fall, Chairman Quigley and Representative Katko invited me to demonstrate such an attack at a briefing on Capitol Hill. I brought a touch-screen voting machine used in 18 states, and we held a small mock election. I remotely hacked the voting machine to steal both Congressmen's votes and changed the election winner.[4]

---

[1] Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections", January 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf
[2] U.S. Senate Select Committee on Intelligence, "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations", 2018. https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf
[3] My curriculum vitae and research publications are available online at https://alexhalderman.com.
[4] I demonstrated a similar attack for *The New York Times*, as shown in this video: https://www.nytimes.com/video/opinion/100000005790489/i-hacked-an-election-so-can-the-russians.html



This level of vulnerability is endemic throughout our election system. Cybersecurity experts have studied a wide range of U.S. voting machines, and in every case, we've found problems that would allow attackers to sabotage machines and alter vote tallies.[5]

Some people think that the decentralized nature of the U.S. voting system and the fact that voting machines aren't directly connected to the Internet make interfering in a state or national election impossible. Unfortunately, that isn't true. Some election functions are actually quite centralized, and our election infrastructure is not as distant from the Internet as it may seem.

Before every election, voting machines and optical scanners need to be programmed with the design of the ballot, the races, and candidates. Election workers create this programming on a central computer called an election management system, then transfer it to voting machines using USB sticks or memory cards. Hackers who compromise an election management system can hijack the ballot programming process to spread a voter-stealing attack to large numbers of machines.

Election management systems are often not adequately protected, and they are not always properly isolated from the Internet. Moreover, a small number of election technology vendors and support contractors program and operate election management systems used by many local governments. The largest of these services over 2000 jurisdictions spread across 34 states. Attackers could target one or a few of these companies and spread an attack to election equipment that serves millions of voters.

Furthermore, in close elections, decentralization can work against us. An attacker can probe the most important swing states or swing districts for vulnerabilities, find the areas that have the weakest protection, and strike there. In a close election, changing a few votes may be enough to tip the result, and attackers can choose where—and on which equipment—to steal those votes.

Fortunately, we know how to better defend election infrastructure and protect it from cyberattacks in 2020 and beyond. There are three essential measures:

1. First, we need to replace obsolete and vulnerable voting equipment, such as paperless systems, with optical scanners and paper ballots—a technology that 30 states already use statewide. Paper ballots provide a resilient physical record of the vote that simply can't be compromised by a cyberattack.

2. Second, we need to consistently check that our election results are accurate, by inspecting enough paper ballots to tell whether the computer results from the optical scanners are right. This can be done with what's known as a risk-limiting audit (RLA). Such audits are a common-sense quality control. By manually checking a random sample of the ballots, officials can quickly and affordably provide high assurance that the election outcome is correct.

---

[5] For an accessible introduction to election cybersecurity, see my online course, *Securing Digital Democracy*, which is available for free on Coursera: https://www.coursera.org/learn/digital-democracy.

3. Lastly, we need to raise the bar for attacks of all sorts—including both vote tampering and sabotage—by applying cybersecurity best practices to the design of voting equipment and registration systems and to the operation of computer systems at election offices.

These are not simply my recommendations.[6] Paper ballots, manual audits, and security best practices are a prescription endorsed by the overwhelming majority of election security experts, and by the National Academies of Science, Engineering, and Medicine.[7,8] These measures are also widely favored by election officials.

Many states have begun to implement these improvements using the $380 million in election cybersecurity funding that Congress appropriated last year. According to the Election Assistance Commission, states intend to use 36% of this funding ($136 million) for cybersecurity improvements, 28% ($103 million) for purchasing new voting equipment, and 6% ($21 million) for improving election audits.[9] These are necessary, appropriate, and urgent priorities.

However, much more needs to be done before Americans go to the polls in 2020. Although some states have made significant progress towards securing their election infrastructure, other have barely gotten started, and the nation as whole remains a patchwork of strength and weakness.

In 2018, 41 states used voting machines that were at least a decade old, and some, including parts of Pennsylvania and New Jersey, used machines dating from around 1990. Forty-three states used machines that are no longer manufactured, forcing election officials to cannibalize old machines for spare parts or even turn to eBay. Twelve states[10] still make widespread use of paperless direct-recording electronic (DRE) voting machines, which are impossible to reliably audit to detect potential errors or malfeasance. All of Georgia, for example, voted in November using the same model of vulnerable paperless DRE that I hacked in front of Chairman Quigley last fall. After years of underinvestment, America's election infrastructure is crumbling, and the $380 million can only serve as a down payment towards fixing it.

Many states would like to replace vulnerable and obsolete voting equipment before 2020, but they are struggling to figure out how to pay for it. Pennsylvania, for instance, plans to switch from insecure paperless machines to paper ballots, but the state's share of last year's HAVA

---

[6] President Trump himself has consistently endorsed the use of paper ballots, both as a candidate and since taking office. He made the point well in 2016: "There's something really nice about the old paper-ballot system. You don't worry about hacking." http://www.businessinsider.com/donald-trump-election-day-fox-news-2016-11

[7] National Academies of Science, Engineering, and Medicine, "Securing the Vote: Protecting American Democracy", 2018. https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

[8] Additionally, the National Institute of Standards and Technology (NIST) has concluded that it is not possible to effectively audit a voting system to detect and correct potential hacking without a voter-verified paper ballot.

[9] U.S. Election Assistance Commission, "EAC Releases 48 HAVA Grants State Plans, Budgets," August 2018. https://www.eac.gov/news/2018/08/21/state--territories-plan-to-spend-majority-of-hava-grant-funds-on-election-security-system-upgrades/

[10] The twelve states with large numbers of paperless DRE voting machines are: Delaware, Georgia, Indiana, Kansas, Kentucky, Louisiana, Mississippi, New Jersey, Pennsylvania, South Carolina, Tennessee, and Texas. Eight additional states use DREs with a voter-verifiable paper audit trail (VVPAT), an obsolete kind of paper backup: Arkansas, California, Illinois, Ohio, North Carolina, Utah, West Virginia, and Wyoming. Verified Voting maintains an online database of the equipment in use in each locality: https://www.verifiedvoting.org/verifier/.

funds was $13.5 million, only about 25% of the cost of implementing hand-marked paper ballots across the state. Georgia's share was $10.3 million, less than a third of what it needs just to replace its paperless machines. Without further federal assistance, we risk that new equipment and other critical improvements won't be in place for many years. With the 2020 election on the horizon—the next major target for foreign cyberattacks—we need to act before it's too late.

What will it cost to fix the problem? The highest priority should be to replace DRE voting equipment nationwide with robustly auditable paper ballots.[11] This would cost about $370 million, assuming an average of $7500 per precinct to acquire one ballot scanner and one accessible voting device.[12] Under HAVA, funds are allocated to states mainly in proportion to voting-age population, rather than by type of existing equipment. If future funding were provided under the existing HAVA formula, I estimate that about $900 million in further appropriations would be needed to ensure that every state with DREs received at least 50% of the funds needed to replace them with hand-marked paper ballots and accessibility devices.

It's important to understand that states can choose from several kinds of voting equipment, and that these choices greatly affect the overall cost and the security achieved. Fortunately, the most cost effective approach is also the most secure: hand-marked paper ballots counted using optical scanners.[13] Some localities are opting instead to purchase ballot-marking devices (BMDs), touchscreen computers that voters use to mark and print their ballots. Equipping a precinct with BMDs for all voters costs about three times as much as using hand-marked paper ballots and providing a dedicated accessibility device for voters with disabilities, and it's also less robust to cyberattacks that render the equipment inoperable. Moreover, it has yet to be established whether voters can reliably detect errors on BMD-printed ballots—which means that fraud could go undetected if the BMDs are hacked to cause them to sometimes print the wrong selections.

In many states, there are no rules in place to prevent local governments from spending federal funds on insecure and unauditable kinds of voting equipment. Some voting machine vendors continue to market paperless DREs, as well as DREs with so-called "voter-verifiable paper audit trails" (VVPATs)—a roll of paper behind a pane of glass that briefly shows the voter's selections. VVPATs are badly inferior to paper ballots, because the printouts are difficult for voters to read and challenging for election officials to effectively audit. Localities purchasing new DREs, whether or not they are equipped with VVPATs, will make it more difficult for states to implement risk-limiting audits statewide. To ensure that taxpayer money is well spent, Congress should prohibit federal funds from being used to purchase voting equipment that does not provide a robustly auditable paper ballot.

---

[11] Once paper ballots are in place, other vital security measures, such as performing risk-limiting audits, are relatively inexpensive to implement. I estimate that performing risk-limiting audits in all federal races nationally would cost less than $25 million per year on average.

[12] For additional cost estimate data, see: Brennan Center and Verified Voting, "Federal Funds for Election Security: Will They Cover the Cost of Voter Marked Paper Ballots?", March 2018. https://www.brennancenter.org/sites/default/files/analysis/Federal_ Funds_for_Election_Security_analysis.pdf

[13] Under HAVA, each polling place must also be equipped with an accessible device to assist voters with disabilities in filling out their ballots.

Election cybersecurity is an urgent matter of national security. Under our time-honored system, implementing the necessary defenses falls to states and local governments. We must not leave them to face the threat of powerful foreign adversaries unaided. Congress should provide for the common defense by equipping states with the resources they need to deploy robustly auditiable paper ballots, risk-limiting audits, and other cybersecurity improvements. With your leadership, elections in 2020 and beyond can be well secured, and voters will have good reason to have confidence in the results. But if we delay action, I fear it is only a matter of time until a national election result is disrupted or stolen in a cyberattack.

U.S. Senate Select Committee on Intelligence

Russian Interference in the 2016 U.S. Elections

Expert Testimony by
J. Alex Halderman
Professor of Computer Science, University of Michigan

June 21, 2017

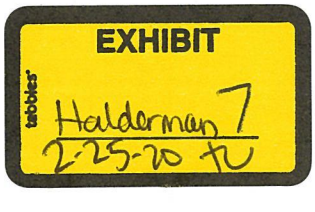
Chairman Burr, Vice Chairman Warner, and members of the Committee, thank you for inviting me to speak today about the security of U.S. elections. I'm here to tell you not just what I think, but about concerns shared by hundreds of experts from across cybersecurity research and industry. Such expertise is relevant because elections—the bedrock of our democracy—are now on the front lines of cybersecurity, and they face increasingly serious threats. Our interest in this matter is decidedly non-partisan; our focus is on the integrity of the democratic process, and the ability of the voting system to record, tabulate, and report the results of elections accurately.

My research in computer science and cybersecurity tackles a broad range of security challenges.[1] I study attacks and defenses for the Internet protocols we all rely on every day to keep our personal and financial information safe. I also study the capabilities and limitations of the world's most powerful attackers, including sophisticated criminal gangs and hostile nation states. A large part of my work over the last ten years has been studying the computer technology that our election system relies on.[2] In this work, I often lead the "red team," playing the role of a potential attacker to find where systems and practices are vulnerable and learn how to make them stronger.

I know firsthand how easy it can be to manipulate computerized voting machines. As part of security testing, I've performed attacks on widely used voting machines, and I've had students successfully attack machines under my supervision.

---

[1] My curriculum vitae and research publications are available online at https://jhalderm.com.
[2] For an accessible introduction to the security risks and future potential of computer voting technologies, see my online course, *Securing Digital Democracy*, which is available for free on Coursera: https://www. coursera.org/learn/digital-democracy.



U.S. Voting Machines Are Vulnerable

As you know, states choose their own voting technology.[3] Today, the vast majority of votes are cast using one of two computerized methods. Most states and most voters use the first type, called optical scan ballots, in which the voter fills out a paper ballot that is then scanned and counted by a computer. The other widely used approach has voters interact directly with a computer, rather than marking a choice on paper. It's called DRE, or direct-recording electronic, voting. With DRE voting machines, the primary records of the vote are stored in computer memory.[4]

Both optical scanners and DRE voting machines are computers. Under the hood, they're not so different from your laptop or smartphone, although they tend to use much older technology—sometimes decades out of date.[5] Fundamentally, they suffer from security weaknesses similar to those of other computer devices. I know because I've developed ways to attack many of them myself as part of my research into election security threats.

Ten years ago, I was part of the first academic team to conduct a comprehensive security analysis of a DRE voting machine. We examined what was at that time the most widely used touch-screen DRE in the country,[6] and spent several months probing it for vulnerabilities. What we found was disturbing: we could reprogram the machine to invisibly cause any candidate to win. We also created malicious software—vote-stealing

---

[3] In many states, the technology in use even differs from county to county. Verified Voting maintains an online database of the equipment in use in each locality: https://www.verifiedvoting.org/verifier/.

[4] Some DREs also produce a printed record of the vote and show it briefly to the voter, using a mechanism called a voter-verifiable paper audit trail, or VVPAT. While VVPAT records provide a physical record of the vote that is a valuable safeguard against cyberattacks, research has shown that VVPAT records are difficult to accurately audit and that voters often fail to notice if the printed record doesn't match their votes. For these reasons, most election security experts favor optical scan paper ballots. See: S. Goggin and M. Byrne, "An Examination of the Auditability of Voter Verified Paper Audit Trail (VVPAT) Ballots." In *Proceedings of the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop*, August 2007. Available at: http://www.accurate-voting.org/wp-content/uploads/2007/08/evt07-goggin.pdf. See also: B. Campbell and M. Byrne, "Now Do Voters Notice Review Screen Anomalies?" In *Proceedings of the 2009 USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop*, August 2009. Available at: http://chil.rice.edu/research/pdf/CampbellByrne_EVT_(2009).pdf.

[5] In 2016, 43 states used computer voting machines that were at least 10 years old—close to the end of their design lifespans. Older hardware and software generally lacks defenses that guard against more modern attack techniques. See: L. Norden and C. Famighetti, "America's Voting Machines at Risk," Brennan Center, 2015. https://www.brennancenter.org/publication/americas-voting-machines-risk. See also: S. Checkoway, A. Feldman, B. Kantor, J. A. Halderman, E. W. Felten, and H. Shacham, "Can DREs Provide Long-Lasting Security? The Case of Return-Oriented Programming and the AVC Advantage." In *Proceedings of the 2009 USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop*, August 2009. Available at: https://jhalderm.com/pub/papers/avc-evt09.pdf.

[6] The machine was the Diebold AccuVote TS, which is still used statewide in Georgia in 2017.

code—that could spread from machine-to-machine like a computer virus, and silently change the election outcome.[7]

Vulnerabilities like these are endemic throughout our election system. Cybersecurity experts have studied a wide range of U.S. voting machines—including both DREs and optical scanners—and in *every single case,* they've found severe vulnerabilities that would allow attackers to sabotage machines and to alter votes.[8] That's why there is overwhelming consensus in the cybersecurity and election integrity research communities that our elections are at risk.

Cyberattacks Could Compromise Elections

Of course, interfering in a state or national election is a bigger job than just attacking a single machine. Some say the decentralized nature of the U.S. voting system and the fact that voting machines aren't directly connected to the Internet make changing a state or national election outcome impossible. Unfortunately, that is not true.[9]

Some election functions are actually quite centralized. A small number of election technology vendors and support contractors service the systems used by many local governments. Attackers could target one or a few of these companies and spread malicious code to election equipment that serves millions of voters.

Furthermore, in close elections, decentralization can actually work against us. An attacker can probe different areas of the most important "swing states" for vulnerabilities, find the areas that have the weakest protection, and strike there.[10] In a close election, changing a few votes may be enough to tip the result, and an attacker can choose where—and on which equipment—to steal those votes. State and local elections are also at risk.

---

[7] A. J. Feldman, J. A. Halderman, and E. W. Felten, "Security Analysis of the Diebold AccuVote-TS Voting Machine." In *Proceedings of the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop* (EVT), August 2007. The research paper and an explanatory video are available at: https://citp.princeton.edu/research/voting/.

[8] For a partial bibliography of voting machine attack research, see: J. A Halderman, "Practical Attacks on Real-world E-voting." In F. Hao and P. Y. A. Ryan (eds.), *Real-World Electronic Voting: Design, Analysis and Deployment*, CRC Press, December 2016. Available at: https://jhalderm.com/pub/papers/ch7-evoting-attacks-2016.pdf.

[9] I explained how attackers can bypass these obstacles in a recent congressional briefing: *Strengthening Election Cybersecurity*, May 15, 2017. The video is available at https://www.electiondefense.org/congressional-briefings-cyber-security/.

[10] For a more detailed description of how adversaries might select targets, see J. A. Halderman, "Want to Know if the Election was Hacked? Look at the Ballots," November 2016, available at: medium.com/@jhalderm/want-to-know-if-the-election-was-hacked-look-at-the-ballots-c61a6113b0ba.

Our election infrastructure is not as distant from the Internet as it may seem.[11] Before every election, voting machines need to be programmed with the design of the ballot, the races, and candidates. This programming is created on a desktop computer called an election management system, or EMS, and then transferred to voting machines using USB sticks or memory cards. These systems are generally run by county IT personnel or by private contractors.[12] Unfortunately, election management systems are not adequately protected, and they are not always properly isolated from the Internet. Attackers who compromise an election management system can spread vote-stealing malware to large numbers of machines.[13]

Russian Attack Attempts: The Threats Are Real

The key lesson from 2016 is that hacking threats are real.

This month, we've seen reports detailing Russian efforts to target voter registration systems in up to 39 states[14] and to develop a capability to spread an attack from an election technology vendor to local election offices.[15] Attacking the IT systems of

---

[11] Fortunately, the U.S. has resisted widespread use of Internet voting—a development that would paint a fresh bull's eye on our democratic system. I myself have demonstrated attacks against Internet voting systems in Washington, D.C., Estonia, and Australia. See:
S. Wolchok, E. Wustrow, D. Isabel, and J. A. Halderman, "Attacking the Washington, D.C. Internet Voting System." In *Proceedings of the 16th Intl. Conference on Financial Cryptography and Data Security*, February 2012. Available at: https://jhalderm.com/pub/papers/dcvoting-fc12.pdf.
D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. Halderman, "Security Analysis of the Estonian Internet Voting System." In *Proceedings of the 21st ACM Conference on Computer and Communications Security* (CCS), November 2014. Available at: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf.
J. A. Halderman and V. Teague, "The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election." In *Proceedings of the 5th International Conference on E-voting and Identity*, September 2015. Available at: https://arxiv.org/pdf/1504.05646v2.pdf.
For a broader discussion of why secure Internet voting systems are likely decades away, see:
R. Cunningham, M. Bernhard, and J. A. Halderman, "The Security Challenges of Online Voting Have Not Gone Away." IEEE Spectrum, November 3, 2016. http://spectrum.ieee.org/tech-talk/telecom/security/the-security-challenges-of-online-voting-have-not-gone-away.

[12] In my own state, Michigan, about 75% of counties outsource pre-election programming to a pair of independent service providers. These are small companies with 10–20 employees that are primarily in the business of selling election supplies, including ballot boxes and "I Voted" stickers.

[13] See, for example, J. Calandrino, et al., "Source Code Review of the Diebold Voting System," part of the California Secretary of State's "Top-to-Bottom" Voting Systems Review, July 2007. Available at: https://jhalderm.com/pub/papers/diebold-ttbr07.pdf.

[14] M. Riley and J. Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known." *Bloomberg*, June 13, 2017. https://www.bloomberg.com/politics/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.

[15] M. Cole, R. Esposito, S. Biddle, and R. Grim, "Top-secret NSA Report Details Russian Hacking Efforts Days Before 2016 Election." *The Intercept*, June 5, 2017. https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.

vendors and municipalities could put the Russians in a position to sabotage equipment on election day, causing voting machines or electronic poll books to fail, resulting in long lines or other disruptions. The Russians could even have engineered this chaos to have a partisan effect, by targeting localities that lean heavily towards one candidate or another.

Successful infiltration of election IT systems also could have put the Russians in a position to spread an attack to the voting machines and potentially steal votes. Although the registration systems involved were generally maintained at the state level, and most pre-election programming is performed by counties or outside vendors, counties tend to be even less well defended than state governments. They typically have few IT support staff and little, if any, cybersecurity expertise.

Another approach that the Russians might have been planning is to tamper with the voting system in an obvious, easily discovered way, such as causing reporting systems to send the news media incorrect initial results on election night. Even if the problem was corrected and no actual votes were changed, this would cause uncertainty in the results and widespread distrust of the system, which would injure our democratic processes. If voters cannot trust that their votes are counted honestly, they will have reason to doubt the validity of elections.[16]

I don't know how far the Russians got in their effort to penetrate our election infrastructure, nor whether they interfered with equipment on election day. (As far as the public knows, no voting equipment has been forensically examined to check whether it was successfully attacked.) But there is no doubt that Russia has the technical ability to commit widescale attacks against our voting system, as do other hostile nations. As James Comey testified here two weeks ago, we know "They're coming after America," and "They'll be back."[17]

Practical Steps to Defend Election Infrastructure

We must start preparing now to better defend our election infrastructure and protect it from cyberattacks before the elections in 2018 and 2020. The good news is, we know how to accomplish this. Paper ballots, audits, and other straightforward steps can make elections much harder to attack.

---

[16] See, as one example, E. H. Spafford, "Voter Assurance." NAE *The Bridge*, December 2008. https://www.nae.edu/19582/Bridge/VotingTechnologies/VoterAssurance.aspx.

[17] Testimony of former FBI Director James B. Comey before the Senate Select Committee on Intelligence, June 8, 2017.

I have entered into the record a letter from over 100 computer scientists, security experts, and election officials. This letter recommends three essential measures that can safeguard U.S. elections:

- First, we need to replace obsolete and vulnerable voting machines, such as paperless systems, with optical scanners and paper ballots—a technology that 36 states already use. Paper provides a resilient physical record of the vote[18] that simply can't be compromised by a cyberattack. President Trump made this point well shortly before the election in an interview with Fox News. "There's something really nice about the old paper-ballot system," he said. "You don't worry about hacking. You don't worry about all the problems that you're seeing."[19]

- Second, we need to consistently and routinely check that our election results are accurate, by inspecting enough of the paper ballots to tell whether the computer results are right.[20] This can be done with what's known as risk-limiting audits.[21] Such audits are a common-sense quality control.[22] By manually checking a relatively small random sample of the ballots, officials can quickly and affordably provide high assurance that the election outcome was correct.

Optical scan ballots paired with risk-limiting audits provide a practical way to detect and correct vote-changing cyberattacks. They may seem low-tech, but they are a reliable, cost-effective defense.[23]

---

[18] Of course, paper ballots can be tampered with too, by people handling them. Optical scan tabulation has the advantage that it produces both paper and electronic records. As long as officials check that both sets of records agree, it would be very difficult for criminals to alter the election outcome without being detected, whether by a cyberattack or by old-fashioned ballot manipulation.

[19] See: http://www.businessinsider.com/donald-trump- election-day-fox-news-2016-11.

[20] At least 29 states already require some form of post-election audit. However, since the procedures in most states are not designed as a cyber defense, the number of ballots that are audited may be much too low or geographically localized to reliably detect an attack. Some states also allow auditing by rescanning paper ballots through the same potentially compromised machines. Results from paperless DRE voting machines cannot be strongly audited, since there is no physical record to check. For state-by-state details, see National Conference of State Legislatures, "Post-election Audits," June 2017. Available at: http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx.

[21] For a detailed explanation of risk-limiting audits, see J. Bretschneider et al., "Risk-Limiting Post-Election Audits: Why and How." Available at: https://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf. New Mexico already requires something similar to a risk-limiting audit, and Colorado is implementing risk-limiting audits starting in 2017. Risk-limiting audits have been tested in real elections in California, Colorado, and Ohio.

[22] One of the reasons why post-election audits are essential is that pre-election "logic and accuracy" testing can be defeated by malicious software running on voting machines. Vote-stealing code can be designed to detect when it's being tested and refuse to cheat while under test. Volkswagen's emission-control software did something similar to hide the fact that it was cheating during EPA tests.

[23] Former CIA director James Woolsey and Lt. Col. Tony Shaffer call for paper ballots and auditing in a May 12, 2017 op-ed in Fox News: "Ultimately, we believe the solution to election insecurity lies in

- Lastly, we need to raise the bar for attacks of all sorts—including both vote tampering and sabotage—by conducting comprehensive threat assessments and by applying cybersecurity best practices to the design of voting equipment[24] and the management of elections.

These fixes aren't expensive. Replacing insecure paperless systems nationwide would cost between $130 million and $400 million.[25] Running risk-limiting audits nationally for federal elections would cost less than $20 million a year.[26] These amounts are vanishingly small compared to the national security improvement the investment buys. Yet such measures could address a prime cyber challenge, boost voter confidence, and significantly strengthen a crucial element of our national security. They would also send a firm response to any adversaries contemplating interfering with our election system.

Election officials have an extremely difficult job, even without having to worry about cyberattacks by hostile governments. The federal government can make prudent and cost-effective investments to help them defend our election infrastructure and uphold voters' confidence. With leadership from across the aisle, and action in partnership with the states, our elections can be well protected in time for 2018 and 2020.

Thank you for the opportunity to testify. I look forward to answering any questions.

President Reagan's famous old adage: 'trust but verify'." http://www.foxnews.com/opinion/2017/05/12/america-s-voting-systems-need-security-upgrades-it-s-time-to-beef-up-cybersecurity.html.

[24] One notable effort to develop secure voting equipment is STAR-Vote, a collaboration between security researchers and the Travis County, Texas elections office. STAR-Vote integrates a range of modern defenses, including end-to-end cryptography and risk limiting audits. See S. Bell et al., "STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System." USENIX Journal of Election Technology and Systems (JETS) 1(1), August 2013. https://www.usenix.org/system/files/conference/evtwote13/jets-0101-bell.pdf.

[25] Brennan Center, "Estimate for the Cost of Replacing Paperless, Computerized Voting Machines," June 2017. https://www.brennancenter.org/sites/default/files/analysis/New_Machines_Cost_Across_Paperless_Jurisdictions%20%282%29.pdf. This cost might be significantly reduced by developing voting equipment based on open-source software and commercial off-the-shelf (COTS) hardware.

[26] This estimate assumes that auditing a federal race will have an average cost similar to manually recounting 10% of precincts. In a risk-limiting audit, the actual number of ballots that must be checked varies with, among other factors, the margin of victory.

[redacted] [redacted]
COMMITTEE SENSITIVE - RUSSIA INVESTIGATION ONLY

116TH CONGRESS *1st Session* | SENATE | REPORT 116-XX

REPORT

OF THE

SELECT COMMITTEE ON INTELLIGENCE

UNITED STATES SENATE

ON

RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION

VOLUME 1: RUSSIAN EFFORTS AGAINST ELECTION INFRASTRUCTURE

WITH ADDITIONAL VIEWS

CONTENTS

Russian Efforts Against Election Infrastructure

I. (U) INTRODUCTION

(U) From 2017 to 2019, the Committee held hearings, conducted interviews, and reviewed intelligence related to Russian attempts in 2016 to access election infrastructure. The Committee sought to determine the extent of Russian activities, identify the response of the U.S. Government at the state, local, and federal level to the threat, and make recommendations on how to better prepare for such threats in the future. The Committee received testimony from state election officials, Obama administration officials, and those in the Intelligence Community and elsewhere in the U.S. Government responsible for evaluating threats to elections.

II. (U) FINDINGS

1. [redacted] The Russian government directed extensive activity, beginning in at least 2014 and carrying into at least 2017, against U.S. election infrastructure[1] at the state and local level. [redacted] The Committee has seen no evidence that any votes were changed or that any voting machines were manipulated.[2]

2. [redacted]

[1] (U) The Department of Homeland Security (DHS) defines *election infrastructure* as "storage facilities, polling places, and centralized vote tabulation locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments, " according to the January 6, 2017 statement issued by Secretary of Homeland Security Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, available at https://www.dhs.gov/news/2017/10/06/statement-secretary-johnson-designation-election-infrastructure-critical. Similarly, the Help America Vote Act (HAVA), Pub. L. No. 107-252, Section 301(b)(1) refers to a functionally similar set of equipment as "voting systems," although the definition excludes physical polling places themselves, among other differences, 52 U.S.C. §21081(b). This report uses the term *election infrastructure* broadly, to refer to the equipment, processes, and systems related to voting, tabulating, reporting, and registration.

[2] [redacted] The Committee has reviewed the intelligence reporting underlying the Department of Homeland Security (DHS) assessment from early 2017 [redacted] The Committee finds it credible.

[3] (U) The names of the states the Committee spoke to have been replaced with numbers. DHS and some states asked the Committee to protect state names before providing the Committee with information. The Committee's goal was to get the most information possible, so state names are anonymized throughout this report. Where the report refers to public testimony by Illinois state election officials, that state is identified.

3. (U) While the Committee does not know with confidence what Moscow's intentions were, Russia may have been probing vulnerabilities in voting systems to exploit later. Alternatively, Moscow may have sought to undermine confidence in the 2016 U.S. elections simply through the discovery of their activity.

4. (U) Russian efforts exploited the seams between federal authorities and capabilities, and protections for the states. The U.S. intelligence apparatus is, by design, foreign-facing, with limited domestic cybersecurity authorities except where the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) can work with state and local partners. State election officials, who have primacy in running elections, were not sufficiently warned or prepared to handle an attack from a hostile nation-state actor.

5. (U) DHS and FBI alerted states to the threat of cyber attacks in the late summer and fall of 2016, but the warnings did not provide enough information or go to the right people. Alerts were actionable, in that they provided malicious Internet Protocol (IP) addresses to information technology (IT) professionals, but they provided no clear reason for states to take this threat more seriously than any other alert received.

6. (U) In 2016, officials at all levels of government debated whether publicly acknowledging this foreign activity was the right course. Some were deeply concerned that public warnings might promote the very impression they were trying to dispel—that the voting systems were insecure.

7. (U) Russian activities demand renewed attention to vulnerabilities in U.S. voting infrastructure. In 2016, cybersecurity for electoral infrastructure at the state and local level was sorely lacking; for example, voter registration databases were not as secure as they could have been. Aging voting equipment, particularly voting machines that had no paper record of votes, were vulnerable to exploitation by a committed adversary. Despite the focus on this issue since 2016, some of these vulnerabilities remain.

8. (U) In the face of this threat and these security gaps, DHS has redoubled its efforts to build trust with states and deploy resources to assist in securing elections. Since 2016, DHS has made great strides in learning how election procedures vary across states and how federal entities can be of most help to states. The U.S. Election Assistance Commission (EAC), the National Association of Secretaries of State (NASS), the National Association of State Election Directors (NASED), and other groups have helped DHS in this effort. DHS's work to bolster states' cybersecurity has likely been effective, in particular for those states that have leveraged DHS's cybersecurity assessments for election infrastructure, but much more needs to be done to coordinate state, local, and federal knowledge and efforts in order to harden states' electoral infrastructure against foreign meddling.

9. (U) To assist in addressing these vulnerabilities, Congress in 2018 appropriated $380 million in grant money for the states to bolster cybersecurity and replace vulnerable

voting machines.[4] When those funds are spent, Congress should evaluate the results and consider an additional appropriation to address remaining insecure voting machines and systems.

10. **(U)** DHS and other federal government entities remain respectful of the limits of federal involvement in state election systems. States should be firmly in the lead for running elections. The country's decentralized election system can be a strength from a cybersecurity perspective, but each operator should be keenly aware of the limitations of their cybersecurity capabilities and know how to quickly and properly obtain assistance.

III. (U) THE ARC OF RUSSIAN ACTIVITIES

[redacted] In its review of the 2016 elections, the Committee found no evidence that vote tallies were altered or that voter registry files were deleted or modified, though the Committee and IC's insight into this is limited. Russian government-affiliated cyber actors conducted an unprecedented level of activity against state election infrastructure in the run-up to the 2016 U.S. elections [redacted] Throughout 2016 and for several years before, Russian intelligence services and government personnel conducted a number of intelligence-related activities targeting the voting process. [redacted] the Committee found ample evidence to suggest that the Russian government was developing and implementing capabilities to interfere in the 2016 elections, including undermining confidence in U.S. democratic institutions and voting processes.[5]

[redacted]

- [redacted]

---

[4] **(U)** Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, 132 Stat. 348, 561-562.
[5] **(U)** The Committee has limited information on the extent to which state and local election authorities carried out forensic evaluation of registration databases. These activities are routinely carried out in the context of private sector breaches.
[6] [redacted] FBI LHM, [redacted]
[7] [redacted] FBI LHM, [redacted]
[8] [redacted] DHS Homeland Intelligence Brief, [redacted]
[9] [redacted] FBI LHM, [redacted]

- [redacted]
- [redacted]

[redacted] Evidence of scanning of state election systems first appeared in the summer prior to the 2016 election. In mid-July 2016, Illinois discovered anomalous network activity, specifically a large increase in outbound data, on a Illinois Board of Elections' voter registry website.[12] Working with Illinois, the FBI commenced an investigation.[13] [redacted] The attack resulted in data exfiltration from the voter registration database.[16]

(U) On August 18, 2016, FBI issued an unclassified FLASH[17] to state technical-level experts on a set of [redacted] suspect IP addresses identified from the attack on Illinois's voter registration databases.[18] [redacted] The FLASH product did not attribute the attack to Russia or any other particular actor.[21]

---

[10] (U[redacted]) FBI Electronic Communication, [redacted]
[11] [redacted] FBI LHM, [redacted]
[12] (U) DHS briefing for SSCI staff, March 5, 2018.
[13] (U) SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 113.
[14] (U[redacted]) According to the United States Computer Emergency Readiness Team (US-CERT), an SQL injection is "an [redacted] technique that attempts to subvert the relationship between a webpage and its supporting database, typically in order to trick the database into executing malicious code."
[15] (U) DHS IIR 4 0050006 17, *An IP Address Targeted Multiple U.S. State Government's to Include Election Systems*, October 4, 2016
[16] (U[redacted]) DHS briefing for SSCI staff, March 5, 2018.
[17] (U) FBI FLASH alerts are notifications of potential cyber threats sent to local law enforcement and private industry so that administrators are able to guard their systems against the described threat. FLASHs marked TLP: AMBER are considered sharable with members of the recipients own organization and those with direct need to know.
[18] [redacted] Number T-LD1004-TT, TLP-AMBER, [redacted]
[19] (U) *Ibid.*
[20] (U) *Ibid.*
[21] R[redacted]wned

(U[redacted]) After the issuance of the August FLASH, the Department of Homeland Security (DHS) and the Multi-State-Information Sharing & Analysis Center (MS-ISAC)[22] asked states to review their log files to determine if the IP addresses described in the FLASH had touched their infrastructure. This request for voluntary self-reporting, in conjunction with DHS analysis of NetFlow activity on MS-ISAC internet sensors, identified another 20 states whose networks had made connections to at least one IP address listed on the FLASH.[23] DHS was almost entirely reliant on states to self-report scanning activity.

[redacted] Former Special Assistant to the President and Cybersecurity Coordinator Michael Daniel said, "eventually we get enough of a picture that we become confident over the course of August of 2016 that we're seeing the Russians probe a whole bunch of different state election infrastructure, voter registration databases, and other related infrastructure on a regular basis."[25] Dr. Samuel Liles, Acting Director of the Cyber Analysis Division within DHS's Office of Intelligence and Analysis (I&A), testified to the Committee on June 21, 2017, that "by late September, we determined that internet-connected election-related networks in 21 states were potentially targeted by Russian government cyber actors."[26]

[redacted]

[22] (U) The MS-ISAC is a DHS-supported group dedicated to sharing information between state, local, tribal, and territorial (SLTT) government entities. It serves as the central cybersecurity resource for SLTT governments. Entities join to receive cybersecurity advisories and alerts, vulnerability assessments, incident response assistance, and other services.

[23] (U[redacted]) DHS IIR 4 005 0006, *An IP Address Targeted Multiple U.S. State Governments to Include Election Systems*, October 4, 2016; DHS briefing for SSCI staff, March 5, 2018.

[24] (U) SSCI Transcript of the Interview with John Brennan, Former Director, CIA, held on Friday, June 23, 2017, p. 41.

[25] (U) SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on August 31, 2017, p. 39.

[26] (U) SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 12.

[redacted]

(U) DHS and FBI issued a second FLASH and a Joint Analysis Report in October that flagged [redacted] suspect IP addresses, many unrelated to Russia.[27] DHS briefers told the Committee that they were intentionally over-reporting out of an abundance of caution, given their concern about the seriousness of the threat. DHS representatives told the Committee, "We were very much at that point in a sort of duty-to-warn type of attitude . . . where maybe a specific incident like this, which was unattributed at the time, wouldn't have necessarily risen to that level. But . . . we were seeing concurrent targeting of other election-related and political figures and political institutions . . . [which] led to what would probably be more sharing than we would normally think to do."[28]

[redacted]

[redacted] DHS assessed that the searches, done alphabetically, probably included all 50 states, and consisted of research on "general election-related web pages, voter ID information, election system software, and election service companies."[31]

[redacted]

---

[27] (U[redacted]) FBI FLASH, Alert Number T-LD1005-TT, TLP-AMBER, [redacted]; DHS/FBI JAR-16-20223, *Threats to Federal, State, and Local Government Systems*, October 14, 2016.

[28] (U) SSCI interview with DHS and CTIIC, February 27, 2018, p. 9-10.

[29] [redacted] FBI LHM, [redacted]

[30] [redacted]

[31] [redacted] DHS Homeland Intelligence Brief, *Update:* [redacted]

[32] [redacted] NSA [redacted] DIRNSA, May 5, 2017. This information was not available to the U.S. government until April 2017.

[33] [redacted]

[34] (U) NSA [redacted] DIRNSA, May 5, 2017.

[redacted]

The Russian Embassy placed a formal request to observe the elections with the Department of State, but also reached outside diplomatic channels in an attempt to secure permission directly from state and local election officials.[37] In objecting to these tactics, then-Assistant Secretary of State for European and Eurasian Affairs Victoria Nuland reminded the Russian Ambassador that Russia had refused invitations to participate in the official OSCE mission that was to observe the U.S. elections.[38]

[35] (U) FBI IIR ; FBI IIR
[36] (U) *Ibid.*
[37] (U) DTS 2018-2152, SSCI Interview with Andrew McCabe, Former Deputy Director of the FBI, February 14, 2018, pp. 221-222.
[38] Email, sent November 4, 2016; from ; to: , , , . Subject: Kislyak Protest of FBI Tactics.
[39] (U) NSA DIRNSA, May 5, 2017.
[40] (U) *Ibid.*
[41]
[42]
[43]

(U) The Committee found no evidence of Russian actors attempting to manipulate vote tallies on Election Day, though again the Committee and IC's insight into this is limited.

(U[redacted]) In the years since the 2016 election, awareness of the threat, activity by DHS, and measures at the state and local level to better secure election infrastructure have all shown considerable improvement. The threat, however, remains imperfectly understood. In a briefing before Senators on August 22, 2018, DNI Daniel Coats, FBI Director Christopher Wray, then-DHS Secretary Kirstjen Nielsen, and then-DHS Undersecretary for the National Protection and Programs Division Christopher Krebs told Senators that there were no known threats to election infrastructure. However, Mr. Krebs also said that top election vulnerabilities remain, including the administration of the voter databases and the tabulation of the data, with the latter being a much more difficult target to attack.[44] Relatedly, several weeks prior to the 2018 mid-term election, DHS assessed that "numerous actors are regularly targeting election infrastructure, likely for different purposes, including to cause disruptive effects, steal sensitive data, and undermine confidence in the election."[45]

[redacted]

IV. (U) ELEMENTS OF RUSSIAN ACTIVITIES

A. (U) Targeting Activity

[redacted] Scanning of election-related state infrastructure by Moscow was the most widespread activity the IC and DHS elements observed in the run up to the 2016 election.[48]

- [redacted] In an interview with the Committee, Mr. Daniel stated: "What it mostly looked like to us was reconnaissance. . . . I would have characterized it at the time as sort of conducting the reconnaissance to do the network mapping, to do the topology mapping so

---

[44] (U) DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.
[45] (U[redacted]) Homeland Security Intelligence Assessment: Cyber Actors Continue to Engage in Influence Activities and Targeting of Election Infrastructure, October 11, 2018.
[46] (U) DTS 2019-1368, NIC 2019-01, Intelligence Community Assessment: A Summary of the Intelligence Community Report on Foreign Interference as Directed by Executive Order 13848, March 29, 2019. p. 2-3.
[47] (U) *Ibid.*
[48] (U) SSCI interview of representatives from DHS and CTIIC, February 27, 2018, p. 12.

that you could actually understand the network, establish a presence so you could come back later and actually execute an operation."[49]

- (U) Testifying before the Committee, Dr. Liles characterized the activity as "simple scanning for vulnerabilities, analogous to somebody walking down the street and looking to see if you are home. A small number of systems were unsuccessfully exploited, as though somebody had rattled the doorknob but was unable to get in . . . [however] a small number of the networks were successfully exploited. They made it through the door."[50]

[redacted] DHS and FBI assessments on the number of affected states evolved since 2016. In a joint FBI/DHS intelligence product published in March 2018, and coordinated with the Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), the Department of State, the National Intelligence Council, the National Security Agency (NSA), and the Department of Treasury, DHS and FBI assessed [redacted] that Russian intelligence services conducted activity [redacted][51]

- [redacted] DHS arrived at their initial assessment by evaluating whether the tactics, techniques, and procedures (TTPs) observed were consistent with previously observed Russian TTPs, whether the actors used known Russian-affiliated malicious infrastructure, and whether a state or local election system was the target.[53]

- (U) The majority of information examined by DHS was provided by the states themselves. The MS-ISAC gathered information from states that noticed the suspect IPs pinging their systems. In addition, FBI was working with some states in local field offices and reporting back FBI's findings.

- (U) If some states evaluated their logs incompletely or inaccurately, then DHS might have no indication of whether they were scanned or attacked. As former-Homeland Security Adviser Lisa Monaco told the Committee, "Of course, the law enforcement and the intelligence community is going to be significantly reliant on what the holders and

---

[49] (U) SSCI Transcript of the Interview of Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, p. 44.
[50] (U) SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 13.
[51] [redacted] DHS/FBI Homeland Intelligence Brief, [redacted]
[52] (U) *See* chart, *infra*, for information on successful breaches.
[53] (U) DHS did not count attacks on political parties, political organizations, or NGOs. For example, the compromise of an email affiliated with a partisan State 13 voter registration organization was not included in DHS's count.

owners and operators of the infrastructure sees on its system [sic] and decides to raise their hand."[54]

[redacted] However, both the IC and the Committee in its own review were unable to discern a pattern in the affected states, [redacted]

(U) Mr. Daniel told the Committee that by late August 2016, he had already personally concluded that the Russians had attempted to intrude in all 50 states, based on the extent of the activity and the apparent randomness of the attempts. "My professional judgment was we have to work under the assumption that they've tried to go everywhere, because they're thorough, they're competent, they're good."[55]

[redacted] Intelligence developed later in 2018 bolstered Mr. Daniel's assessment that all 50 states were targeted. [redacted]

- [redacted]

[54] **(U)** SSCI Transcript of the Interview with of Lisa Monaco, Former Homeland Security Advisor, August 10, 2017, p. 38.
[55] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, p. 40.
[56] [redacted] DHS/FBI Homeland Intelligence Bulletin, [redacted]
[57] **(U)** *Ibid.*
[58] **(U)** DHS briefing for SSCI staff, March 5, 2018.
[59] **(U)** SSCI interview of representatives from DHS and CTIIC, February 27, 2018, pp. 11-12.
[60] **(U)** DHS briefing for SSCI staff, March 5, 2018.

- [redacted]
- [redacted]

[redacted]

(U) However, IP addresses associated with the August 18, 2016 FLASH provided some indications the activity might be attributable to the Russian government, particularly the GRU:

- [redacted]
- [redacted]
- (U[redacted]) One of the Netherlands-based [redacted] "exhibited the same behavior from the same node over a period of time. . . . It was behaving like . . . the same user or group of users was using this to direct activity against the same type of targets," according to DHS staff.[69]

---

[61] (U) *Ibid.*
[62] (U) *Ibid.*
[63] (U) *Ibid.*
[64] (U) *Ibid.*
[65] [redacted]
[66] FBI IIR [redacted]
[67] (U) Cyber Threat Intelligence Integration Center (CTIIC) Cyber Threat Intelligence Summary, October 7, 2016.
[68] (U) *Ibid.*
[69] (U) SSCI interview of representatives from DHS and CTIIC, February 27, 2018, p. 13.

- [redacted]

[redacted] The IC's confidence level about the attribution of the attacks evolved over 2017 and into 2018. [redacted]

- [redacted]

- [redacted]

[redacted] The Committee reached out to the 21 states that DHS first identified as targets of scanning activity to learn about their experiences. Election officials provided the Committee

---

[70] (U) DHS Electronic Communication, December 19, 2016, email from: DHS/NCCIC; to: CIA.
[71] [redacted]
[72] [redacted]
[73] [redacted] DHS Intelligence Assessment, *Hostile Russian Cyber Targeting of Election Infrastructure in 2016; Probable Non-State Actors Attempt Disruption*, May 3, 2017.
[74] (U) *Ibid.*
[75] (U) SSCI interview of representatives from DHS and CTIIC, February 27, 2018, p. 13.
[76] [redacted] DHS arrived at their initial assessment of 21 states affected by adding the eleven plus seven states, plus the three where scanning activity appeared directed at less specifically election-focused infrastructure.
[77] (U) SSCI conference call with DHS and FBI, March 29, 2018.

details about the activity they saw on their networks, and the Committee compared that accounting to DHS's reporting of events.[78] Where those accounts differed is noted below. The scanning activity took place from approximately June through September 2016.

STATE	OBSERVED ACTIVITY[79]
Illinois	**(U)** *See infra,* "Russian Access to Election-Related Infrastructure" for a detailed description.
State 2	**(U)** *See infra,* "Russian Access to Election-Related Infrastructure" for a detailed description.
State 3	**(U)** According to State 3 officials, cyber actors using infrastructure identified in the August FLASH conducted scanning activity.[80] State 3 officials noticed "abnormal behavior" and took action to block the related IP addresses.[81] [redacted] DHS reported GRU scanning attempts against two separate domains related to election infrastructure.[82]
State 4	**(U)** *See infra,* "Two Unexplained Events" for a detailed description.
State 5	**(U)** Cyber actors using infrastructure identified in the August FLASH scanned "an old website and non-relevant archives," according to the State 5 Secretary of State's office.[83] The following day, State 5 took action to block the IP address.[84] [redacted] DHS, however, reported GRU scanning activity on two separate State 5 Secretary of State websites, plus targeting of a District Attorney's office[85] in a particular city.[86] Both the websites appear to be current addresses for the State 5 Secretary of State's office.
State 6	**(U)** According to State 6 officials, cyber actors using infrastructure identified in the August FLASH scanned[87] the entire state IT infrastructure, including by using the Acunetix tool, but the "affected systems" were the Secretary of State's

[78] **(U)** DHS briefed Committee staff three times on the attacks, and staff reviewed hundreds of pages of intelligence assessments.

[79] **(U)** Slight variation between what states and DHS reported to the Committee is an indication of one of the challenges in election cybersecurity. The system owners—in this case, state and local administrators—are in the best position to carry out comprehensive cyber reviews, but they often lack the expertise or resources to do so. The federal government has resources and expertise, but the IC can see only limited information about inbound attacks because of legal restrictions on operations inside the United States.

[80] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 3], December 8, 2017.

[81] **(U)** *Ibid.*

[82] **(U)** DHS briefing for Committee staff on March 5, 2018.

[83] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 5], December 1, 2017.

[84] **(U)** *Ibid.*

[85] **(U/**[redacted]**)** Briefers suggested the "most wanted" list housed on the District Attorney's website may have in some way been connected to voter registration. The exact nature of this connection, including whether it was a technical network connection or whether databases of individuals with felony convictions held by the District Attorney's office had voting registration implications, is unclear.

[86] **(U)** DHS briefing for Committee staff on March 5, 2018.

[87] **(U)** State 6 officials did not specify, but in light of the DHS assessment, they likely meant SQL injection.

	web application and the election results website.[88] If the penetration had been successful, actors could have manipulated the unofficial display of the election tallies.[89] State officials believed they would have caught any inconsistency quickly.[90] State 6 became aware of this malicious activity and alerted partners.[91] [redacted] DHS reported that GRU actors scanned State 6, then unsuccessfully attempted many SQL injection attacks. State 6 saw the highest number of SQL attempts of any state.
State 7	(U) According to State 7 officials, cyber actors using infrastructure identified in the August FLASH scanned public-facing websites, including the "static" election site.[92] It seemed the actors were "cataloging holes to come back later," according to state election officials.[93] State 7 became aware of this malicious activity after receiving an FBI alert.[94] [redacted] DHS reported GRU scanning attempts against two separate domains related to election infrastructure.[95]
State 8	(U) According to State 8 officials, cyber actors using infrastructure identified in the August FLASH scanned a State 8 public election website on one day.[96] State 8 officials described the activity as heightened but not particularly out of the ordinary.[97] State 8 became aware of this malicious activity after receiving an alert.[98] [redacted]
State 9	(U) According to State 9 officials, cyber actors using infrastructure identified in an October MS-ISAC advisory[101] scanned the statewide voter registration

[88] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017.
[89] (U) *Ibid.*
[90] (U) *Ibid.*
[91] (U) *Ibid.*
[92] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.
[93] (U) *Ibid.*
[94] (U) *Ibid.*
[95] (U) DHS briefing for Committee staff on March 5, 2018.
[96] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[97] (U) *Ibid.*
[98] (U) *Ibid.*
[99] (U) DHS briefing for Committee staff on March 5, 2018.
[100] (U) *Ibid.*
[101] (U) While the Committee was unable to review the specific indicators shared with State 9 by the MS-ISAC in October, the Committee believes at least one of the relevant IPs was originally named in the August FLASH because of technical data held by DHS which was briefed to the Committee.

	system.[102] Officials used the analogy of a thief casing a parking lot: they said the car thief "didn't go in, but we don't know why."[103] State 9 became aware of this malicious activity after receiving an alert.[104] [redacted] DHS reported GRU scanning activity on the Secretary of State domain.[105]
State 10	**(U)** According to State 10 officials, cyber actors using infrastructure identified in the August FLASH conducted activity that was "very loud," with a three-pronged attack: a Netherlands-based IP address attempted SQL injection on all fields 1,500 times, a U.S.-based IP address attempted SQL injection on several fields, and a Poland-based IP address attempted SQL injection on one field 6-7 times.[106] State 10 received relevant cybersecurity indictors from MS-ISAC in early August, around the same time that the attacks occurred.[107] State 10's IT contractor attributed the attack to Russia and suggested that the activity was reminiscent of other attacks where attackers distract with lots of noise and then "sneak in the back."[108] **(U)** State 10, through its firewall, blocked attempted malicious activity against the online voter registration system and provided logs to the National Cybersecurity and Communications Integration Center (NCCIC)[109] and the U.S. Computer Emergency Readiness Team (US-CERT).[110] State 10 also brought in an outside contractor to assist.[111] [redacted] DHS confirmed GRU SQL injection attempts against State 10's voter services website on August 5 and said that the attack was blocked after one day by State 10's firewall.[112]
State 11	**(U)** According to State 11 officials, they have seen no evidence of scanning or attack attempts related to election infrastructure in 2016.[113] While State 11 officials noted an IP address "probing" state systems, activity which was "broader than state election systems," State 11 election officials did not provide specifics on which systems.[114]

[102] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.
[103] **(U)** *Ibid.*
[104] **(U)** *Ibid.*
[105] **(U)** DHS briefing for Committee staff on March 5, 2018.
[106] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 10], November 29, 2017.
[107] **(U)** *Ibid.*
[108] **(U)** *Ibid.*
[109] **(U)** NCCIC is DHS's cyber watch center.
[110] **(U)** *Ibid.*
[111] **(U)** *Ibid.*
[112] **(U)** DHS briefing for Committee staff on March 5, 2018.
[113] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 11], December 8, 2017.
[114] **(U)** *Ibid.*

	[redacted] DHS reported GRU scanning activity on the Secretary of State domain.[115]
State 12	**(U)** Cyber actors using infrastructure identified in the August FLASH conducted scanning activity that "lasted less than a second and no security breach occurred," according to State 12 officials.[116] State 12 became aware of this malicious activity after being alerted to it.[117] [redacted] DHS reported that because of a lack of sensor data related to this incident, they relied on NetFlow data, which provided less granular information.[118] DHS's only clear indication of GRU scanning on State 12's Secretary of State website came from State 12 self-reporting information to MS-ISAC after the issuance of the August FLASH notification.[119]
State 13	**(U)** According to State 13 officials, they have seen no evidence of scanning or attack attempts related to state-wide election infrastructure in 2016.[120] [redacted]
State 14	[redacted] MS-ISAC passed DHS reports of communications between a suspect IP address used by the GRU at the time and the State 14 election commission webpage, but no indication of a compromise.[123] In addition, DHS was informed of activity relating to separate IP addresses in the August FLASH,

[115] **(U)** DHS briefing for Committee staff on March 5, 2018.
[116] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 12], December 1, 2017.
[117] **(U)** *Ibid.*
[118] **(U)** DHS briefing for Committee staff on March 5, 2018.
[119] **(U)** *Ibid.*
[120] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.
[121] **(U)** FBI IIR [redacted] DHS briefing for Committee staff on March 5, 2018.
[122] [redacted]; DHS briefing for Committee staff on March 5, 2018. For more information on decisions by DHS to exclude certain activity in its count of 21 states, *see* text box, *infra*, "DHS Methodology for Identifying States Touched by Russian Cyber Actors."
[123] [redacted] DHS/FBI Homeland Intelligence Brief, [redacted]; DHS briefing for Committee staff on March 5, 2018.

	including attempted Domain Name System (DNS) lookups and potentially malicious emails, some dating back to January 2016.[124]
State 15	**(U)** State 15 officials were not aware that the state was among those targeted until they were notified.[125] State 15's current lead election official was not in place during the 2016 election so they had little insight into any scanning or attempted intrusion on their systems. State 15 officials said that generally they viewed 2016 as a success story because the attempted infiltration never got past the state's four layers of security. [redacted] DHS reported broad GRU scanning activity on State 15 government domains.[126]
State 16	**(U)** According to State 16 officials, cyber actors using infrastructure identified in the October FLASH conducted scanning activity against a state government network.[127] [redacted] DHS reported information on GRU scanning activity based on a self-report from State 16 after the issuance of the October FLASH.[128]
State 17	**(U)** State 17 officials reported nothing "irregular, inconsistent, or suspicious" leading up to the election.[129] While State 17 IT staff received an MS-ISAC notification, that notification was not shared within the state government.[130] [redacted] DHS reported GRU scanning activity on an election-related domain.[131]
State 18	**(U)** State 18 election officials said they observed no connection from the IP addresses listed in the election-related notifications.[132] [redacted] DHS reported indications of GRU scanning activity on a State 18 government domain.[133]
State 19	**(U)** According to State 19 officials, cyber actors using infrastructure identified in October by MS-ISAC conducted scanning activity. State 19 claimed this activity was "blocked," but did not elaborate on why or how it was blocked.[134]

---

[124] (U//[redacted]) DHS IIR 4 019 0012 17, *Cyber Activity Targeting [State 14] Government Networks from Internet Protocol Addresses Associated with Targeting State Elections Systems*, October 21, 2016.
[125] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 15], March 12, 2018.
[126] (U) DHS briefing for Committee staff on March 5, 2018.
[127] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 16], December 1, 2017.
[128] (U) DHS briefing for Committee staff on March 5, 2018.
[129] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 17], January 25, 2018.
[130] (U) *Ibid.*
[131] (U) DHS briefing for Committee staff on March 5, 2018.
[132] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 18], December 8, 2017.
[133] (U) DHS briefing for Committee staff on March 5, 2018.
[134] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 19], December 1, 2017.

	[redacted] DHS reported indications of GRU scanning activity on two separate State 19 government domains.[135]
State 20	**(U)** According to State 20 officials, cyber actors using infrastructure identified in October by MS-ISAC were "knocking" on the state's network, but no successful intrusion occurred.[136] [redacted] DHS reported GRU scanning activity on the Secretary of State domain.[137]
State 21	**(U)** State 21 officials received indicators from MS-ISAC in October 2016. They said they were not aware the state was among those targeted until notified.[138] [redacted] DHS reported GRU scanning activity on an election-related domain as well as at least one other government system connected to the voter registration system.[139]

[redacted] Neither DHS nor the Committee can ascertain a pattern to the states targeted, lending credence to DHS's later assessment that all 50 states probably were scanned. DHS representatives told the Committee that "there wasn't a clear red state-blue state-purple state, more electoral votes, less electoral votes" pattern to the attacks. DHS acknowledged that the U.S. Government does not have perfect insight, and it is possible the IC missed some activity or that states did not notice intrusion attempts or report them.[140] [redacted]

[redacted]

---

[135] **(U)** DHS briefing for Committee staff on March 5, 2018.
[136] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 20], November 17, 2017.
[137] **(U)** DHS briefing for Committee staff on March 5, 2018.
[138] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 21], November 17, 2017.
[139] **(U)** DHS briefing for Committee staff on March 5, 2018.
[140] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 25.
[141] [redacted]
[142] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 21.

(U/[redacted]) As of October 2018, the IC and DHS were looking for evidence of threats to election systems, [redacted]. An October 11, 2018 DHS Intelligence Assessment reported the following:

> *We judge that numerous actors are regularly targeting election infrastructure, likely for different purposes, including to cause disruptive effects, steal sensitive data, and undermine confidence in the election. We are aware of a growing volume of malicious activity targeting election infrastructure in 2018, although we do not have a complete baseline of prior years to determine relative scale of the activity. Much of our understanding of cyber threats to election infrastructure is due to proactive sharing by state and local election officials, as well as more robust intelligence and information sharing relationships amongst the election community and within the Department. The observed activity has leveraged common tactics—the types of tactics that are available to nation-state and non-state cyber actors, alike—with limited success in compromising networks and accounts. We have not attributed the activity to any foreign adversaries, and we continue to work to identify the actors behind these operations. At this time, all these activities were either prevented or have been mitigated.*

(U/[redacted]) Specifically:

> *Unidentified cyber actors since at least April 2018 and as recently as early October continue to engage in a range of potential elections-related cyber incidents targeting election infrastructure using spear-phishing, database exploitation techniques, and denial of service attacks, possibly indicating continued interest in compromising the availability, confidentiality, and integrity of these systems. For example, on 24 August 2018, cybersecurity officials detected multiple attempts to illegally access the State of Vermont's Online Voter Registration Application (OLVR), which serves as the state's resident voter registration database, according to DHS reporting. The malicious activity included one Cross Site Scripting attempt, seven Structured Query Language (SQL) injection attempts, and one attempted Denial of Service (DoS) attack. All attempts were unsuccessful.*[143]

(U/[redacted]) In summarizing the ongoing threat to U.S. election systems, DHS further said in the same product, "We continue to assess multiple elements of U.S. election infrastructure are potentially vulnerable to cyber intrusions."[144]

B. (U) Russian Access to Election Infrastructure

---

[143] (U/[redacted]) DHS, Homeland Security Intelligence Assessment, *Cyber Actors Continue to Engage in Influence Activities and Targeting of Election Infrastructure*, October 11, 2018.
[144] (U) *Ibid.*

(U) The January 6, 2017 Intelligence Community Assessment (ICA), "Assessing Russian Activities and Intentions in Recent U.S. Elections," states:

> *Russian intelligence obtained and maintained access to elements of multiple U.S. state or local electoral boards. DHS assesses that the types of systems Russian actors targeted or compromised were not involved in vote tallying.*[145]

[redacted] Based on the Committee's review of the ICA, the Committee concurs with this assessment. The Committee found that Russian-affiliated cyber actors gained access to election infrastructure systems across two states, including successful extraction of voter data. However, none of these systems were involved in vote tallying.

1. (U) Russian Access to Election Infrastructure: Illinois

(U) In June 2016, Illinois experienced the first known breach by Russian actors of state election infrastructure during the 2016 election.[146] As of the end of 2018, the Russian cyber actors had successfully penetrated Illinois's voter registration database, viewed multiple database tables, and accessed up to 200,000 voter registration records.[147] The compromise resulted in the exfiltration of an unknown quantity of voter registration data.[148] Russian cyber actors were in a position to delete or change voter data, but the Committee is not aware of any evidence that they did so.[149]

- [redacted] DHS assesses with high confidence that the penetration was carried out by Russian actors.[150]
- (U/[redacted]) The compromised voter registration database held records relating to 14 million registered voters, [redacted]. The records exfiltrated included information on each voter's name, address, partial social security number, date of birth, and either a driver's license number or state identification number.[151]

---

[145] (U) Intelligence Community Assessment, *Assessing Russian Activities and Intentions in Recent U.S. Elections*, January 6, 2017, p. iii.
[146] (U/[redacted]) DHS IIR 4 005 0006, *An IP Address Targeted Multiple U.S. State Government's to Include Election Systems*, October 4, 2016; DHS briefing for SSCI staff, March 5, 2018.
[147] (U) "Illinois election officials say hack yielded information on 200,000 voters," [Local Newspaper], August 29, 2016.
[148] (U) DHS IIR [redacted] SCI Open Hearing on June 21, 2017, p 110
[149] (U) State Board of Elections, *Illinois Voter Registration System Records Breached*, August 31, 2016. As reflected elsewhere in this report, the Committee did not undertake its own forensic analysis of the Illinois server logs to corroborate this statement; SSCI interview with DHS and CTIIC, February 27, 2018, p. 24.
[150] (U) *See infra*, "Russian Scanning and Attempted Access to Election-Related Infrastructure" for a complete discussion on attribution related to the set of cyber activity linked to the infrastructure used in the Illinois breach.
[151] (U/[redacted]) FBI IIR [redacted] DHS Intelligence Assessment, May 3, 2017, 0144-17, p. 2.

- [redacted] DHS staff further recounted to the Committee that "Russia would have had the ability to potentially manipulate some of that data, but we didn't see that."[152] Further, DHS staff noted that "the level of access that they gained, they almost certainly could have done more. Why they didn't . . . is sort of an open-ended question. I think it fits under the larger umbrella of undermining confidence in the election by tipping their hand that they had this level of access or showing that they were capable of getting it."[153]

- **(U)** According to a Cyber Threat Intelligence Integration Center (CTIIC) product, Illinois officials "disclosed that the database has been targeted frequently by hackers, but this was the first instance known to state officials of success in accessing it."[154]

(U) In June 2017, the Executive Director of the Illinois State Board of Elections (SBE), Steve Sandvoss, testified before the Committee about Illinois's experience in the 2016 elections.[155] He laid out the following timeline:

- **(U)** On June 23, 2016, a foreign actor successfully penetrated Illinois's databases through an SQL attack on the online voter registration website. "Because of the initial low-volume nature of the attack, the State Board of Election staff did not become aware of it at first."[156]

- **(U)** Three weeks later, on July 12, 2016, the IT staff discovered spikes in data flow across the voter registration database server. "Analysis of the server logs revealed that the heavy load was a result of rapidly repeated database queries on the application status page of our paperless online voter application website."[157]

- **(U)** On July 13, 2016, IT staff took the website and database offline, but continued to see activity from the malicious IP address.[158]

- **(U)** "Firewall monitoring indicated that the attackers were hitting SBE IP addresses five times per second, 24 hours a day. These attacks continued until August 12th [2016], when they abruptly ceased."[159]

---

[152] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 14.
[153] **(U)** *Ibid.*
[154] **(U)** CTIIC Cyber Threat Intelligence Summary, August 18, 2016.
[155] **(U)** SSCI Open Hearing on June 21, 2017. The Committee notes that, in his testimony, Mr. Sandvoss said Illinois still had not been definitively told that Russia perpetrated the attack, despite DHS's high confidence. The Committee also notes that DHS eventually provided a briefing to states during which DHS provided further information on this topic, including the DHS high-confidence attribution to Russia.
[156] **(U)** *Ibid.*, p. 110.
[157] **(U)** *Ibid.*
[158] **(U)** *Ibid.*, p. 111.
[159] **(U)** *Ibid.*

- **(U)** On July 19, 2016, the election staff notified the Illinois General Assembly and the Attorney General's office.
- **(U)** Approximately a week later, the FBI contacted Illinois.[160]
- **(U)** On July 28, 2016, both the registration system and the online voter registration became fully functional again.[161]

2. (U) Russian Access to Election Infrastructure: State 2

[redacted] Separately, GRU cyber actors breached election infrastructure in State 2. [redacted]

- [redacted]

---

[160] **(U)** *Ibid.*, p. 113.
[161] **(U)** *Ibid.*, p. 112.
[162] **(U)** [redacted] FBI Electronic Communication, [redacted]
[163] **(U)** *Ibid.*
[164] [redacted]
[165] **(U)** FBI Briefing on [State 2] Election Systems, June 25, 2018.
[166] **(U)** DHS briefing for SSCI staff, March 5, 2018.
[167] **(U)** *Ibid.*
[168] **(U)** *Ibid.*
[169] **(U)** *Ibid.*
[170] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 16.
[171] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, compartmented session.

[redacted]

(U) FBI and DHS Interactions with State 2[179]	
August 18, 2016	(U) FBI FLASH notification identified IP addresses targeting election offices.[180]
August 24, 2016	(U) State 2 Department of State received the FLASH from National Association of Secretaries of State.[181]
August 26, 2016	(U) State 2 Department of State forwarded FLASH to counties and advised them to block the IP addresses.[182] [redacted] Separately, [redacted] determined one of the listed IP addresses scanned its system.[183] [redacted] subsequently discovered suspected intrusion activity and contacted the FBI.[184]

[172] (U) *Ibid.*
[173] (U) *Ibid.*
[174] (U) *Ibid.*
[175] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, pp. 7.
[176] (U) *Ibid.*
[177] [redacted] *Ibid. See also* EB-0004893-LED
[178] (U) SSCI interview with DHS and CTIIC, February 27, 2018, p. 42.
[179] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, pp. 7.
[180] (U) FBI FLASH, Alert Number T-LD1004-TT, TLP-AMBER, [redacted]
[181] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 4.
[182] (U) *Ibid.*, pp. 4-5.
[183] (U) *Ibid.*, p. 5.
[184] (U) *Ibid.*

August 31, 2016	[redacted] FBI opened its investigation on the [redacted] and "conducted outreach to State 2 county election officials to discuss individual security postures and any suspicious activity."[185] FBI outreach reveals that one State 2 county—County A—was scanned.[186]
September 30, 2016	[redacted] FBI held a conference call with county election officials to advise of the attempt to probe County A.[187] FBI also notified state and local officials of available DHS services.[188]
October 4, 2016	[redacted] County B's IT administrator contacted FBI regarding a potential intrusion.[189] According to the FBI, "Of particular concern, the activity included a connection to a county voting, testing, and maintenance server used for poll worker classes."[190]
October 14, 2016	(U) FBI shared County B indicators by issuing a FLASH.[191]
December 29, 2016	(U) DHS and FBI released a Joint Analysis Report (JAR) on the "GRIZZLY STEPPE" intrusion set; report represents the first IC attribution of state election-related systems to the Russians.[192]
[redacted]	[redacted]
June 2017	(U) DHS notified State 2 counties of a possible intrusion "as part of a broader notification to 122 entities identified as spearphishing victims in an intelligence report."[194]

[185] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 5.
[186] (U) *Ibid.*
[187] (U) *Ibid.*, pp. 5-6.
[188] (U) *Ibid.*, p. 6.
[189] (U) *Ibid.*
[190] (U) *Ibid.*
[191] (U/[redacted]) FBI FLASH, Alert Number T-LD1005-TT, TLP-AMBER, [redacted]
[192] (U) DHS/FBI, Joint Analysis Report, JAR-16-20296A, GRIZZLY STEPPE – Russian Malicious Cyber Activity, December 29, 2016.
[193] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 7.
[194] (U) *Ibid.*

July 2017	**(U)** FBI published a FLASH report warning of possible spearphishing.[195]
November 2017	**(U)** FBI and DHS participated in the first meeting of the State 2 elections task force.[196]
February 2018	**(U)** FBI requested direct engagement with Counties B, C, and D, including a reminder of available DHS services.[197]
March 2018	**(U)** FBI reports that "our office engaged" the affected counties through the local FBI field office.[198] The FBI could not provide any further detail on the substance of these engagements to the Committee.
May 29, 2018	[redacted] FBI provided a SECRET Letterhead Memo to DHS "formally advising of our investigation into the intrusion [redacted], the reported intrusion at County B, and suspected compromises of Counties C and D."[199]
June 11, 2018	**(U)** FBI reports that as of June 11, 2018, Counties A, B, C, and D had not accepted DHS services.[200]

[redacted]

---

[195] **(U)** FBI FLASH, Alert Number EB-000083-LD, TLP-AMBER, [redacted]. *See* DTS 2018-3174.
[196] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 7.
[197] **(U)** *Ibid.*, p. 6.
[198] **(U)** *Ibid.*, p. 34.
[199] **(U)** *Ibid.*, pp. 8-9.
[200] **(U)** *Ibid.*, p. 20.
[201] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, pp. 20-21.
[202] [redacted] DHS briefing for SSCI staff, March 5, 2018.

- **(U)** State 2's Secretary of State and Election Director told the Committee in December 2017 that there was "never an attack on our systems." "We did not see any unusual activities. I would have known about it personally."[203] State 2 did not want to share with the Committee its cybersecurity posture, but state officials communicated that they are highly confident in the security of their systems.[204]

- **(U)** State 2's election apparatus is highly decentralized, with each county making its own decisions about acquiring, configuring, and operating election systems.[205]

- **(U)** As of August 9, 2018, DHS was complimentary of the steps State 2 had taken to secure its voting systems, including putting nearly all counties on the ALBERT sensor system, joining the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), and using congressionally appropriated funds plus additional state funds to hire cybersecurity advisors.[206]

C. (U) Russian Efforts to Research U.S. Voting Systems, Processes, and Other Elements of Voting Infrastructure

[redacted]

- [redacted]

---

[203] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 2], December 1, 2017.
[204] **(U)** *Ibid.*
[205] **(U)** *Ibid.*
[206] **(U)** DTS 2018-2581, Memorandum for the Record, Telephone call with DHS, August 9, 2018.
[207] [redacted] FBI LHM, [redacted]
[208] **(U)** *Ibid.*, p. 5.
[209] [redacted] Note: "FISA" refers to electronic surveillance collected on a foreign power or an agent of a foreign power pursuant to the Foreign Intelligence Surveillance Act of 1978. This collection could have come from landlines, electronic mail accounts, or mobile phones used by personnel at a foreign embassy (i.e., an "establishment" FISA) or used by personnel associated with a foreign power (i.e., "agents of a foreign power"). This FISA collection would have been approved by the Foreign Intelligence Surveillance Court ("FISC"), effectuated by FBI, and then could also have been shared with NSA or CIA, or both, depending on the foreign target.

- It is unknown if Tarantsov attended the events.

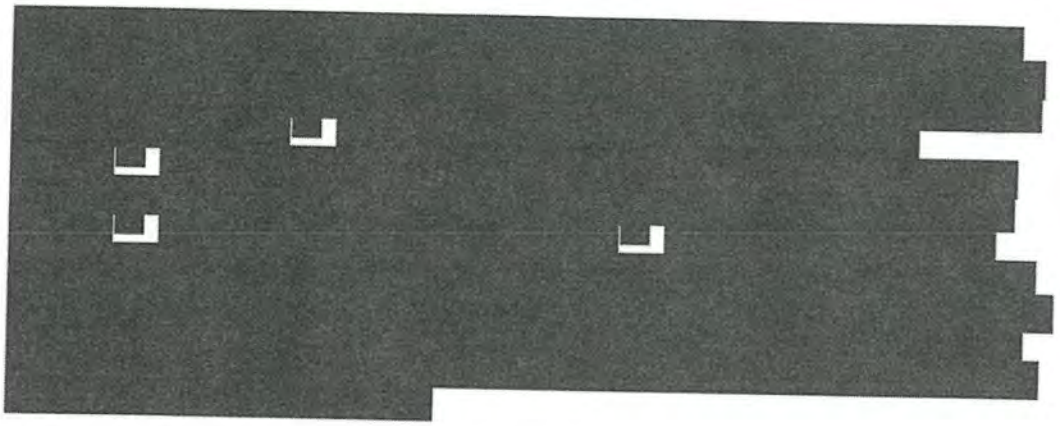
D. (U) Russian Activity Directed at Voting Machine Companies

---

210 FBI LHM,
211 FBI LHM,
212 (U) *Ibid.*
213 (U) *Ibid.*, p. 3.
214 (U) *Ibid.*, p. 4.
215 (U) *Ibid.*
216 (U) *Ibid.*, p. 5.
217

Russian government actors engaged in attacks on election systems,

- FBI reported that "between December 2015 and June 2016, DHS further told the Committee that malicious cyber actors had scanned a widely-used vendor of election systems.[219]



E. (U) Russian Efforts to Observe Polling Places

Department of State were aware that Russia was attempting to send election observers to polling places in 2016. The true intention of these efforts is unknown.

---

[218] FBI Electronic Communication,

[219] (U) DHS briefing for SSCI staff, March 5, 2018.

[220]

[221] (U) *Ibid.*

[222] (U) *Ibid.*

[223] (U) NSA DIRNSA, May 5, 2017, p. 3.

[224] (U) *Ibid.*, pp. 1-3.

[225] (U) FBI IIR

[226] (U) *Ibid.*

- The Russian Embassy placed a formal request to observe the elections with the Department of State, but also reached outside diplomatic channels in an attempt to secure permission directly from state and local election officials.[227] For example, in September 2016, the State 5 Secretary of State denied a request by the Russian Consul General to allow a Russian government official inside a polling station on Election Day to study the U.S. election process, according to State 5 officials.[228]

n mission.[231]

nterfere

-

---

[227] (U) DTS 2018-2152, SSCI Transcript of the Interview of Andrew McCabe, Former Deputy Director of the Federal Bureau of Investigation, February 14, 2018, pp. 221-222.
[228] (U) *Ibid.*
[229] (U) *Ibid.*
[230] (U) *Ibid.*
[231] Email, sent November 4, 2016; from ; to: ; subject: Kislyak Protest of FBI Tactics.
[232] Email, sent: September 13, 2016; from: subject: Russia visas/travel.
[233] (U) *Ibid.*
[234] (U) *Ibid.*
[235] Email Sent: Monday, November 7, 2016, 8:11 AM; from: ; to: subject: RE: Kislyak Protest of FBI Tactics --- SECRET//NOFORN.

F.

G. (U) Russian Activity Possibly Related to a Misinformation Campaign on Voter

---

[236] DTS 2018-3952; MFR of Interview with Randy Coleman, December 5, 2018.
[237] (U) NSA DIRNSA, May 5, 2017.
[238] (U) *Ibid.*
[239] (U) SSCI Interview with DHS and CTIIC, February 27, 2018, pp. 47-48.
[240] FBI IIR
[241] (U/) FBI LHM,
[242] (U) *Ibid.*

[redacted]

(U) The declassified, January 6, 2017, Intelligence Community Assessment also highlighted preparations related to voter fraud, noting that Russian diplomats "were prepared to publicly call into question the validity of the results" and that "pro-Kremlin bloggers had prepared a Twitter campaign, #DemocracyRIP, on election night in anticipation of Secretary Clinton's victory, judging from their social media activity."[245]

(U) During a 2017 election, State 17 saw bot activity on social media, including allegations of voter fraud, in particular on Reddit. State 17 had to try to prove later that there was no fraud.[246]

H. (U) Two Unexplained Events

1. (U) Cyber Activity in State 22

[redacted]

[243] [redacted]
[244]
[245] (U) Intelligence Community Assessment, *Assessing Russian Activities and Intentions in Recent U.S. Elections*, January 6, 2017, p. 2.
[246] (U) *See* Memorandum for the Record, SSCI Staff, Conference Call with State 17, January 25, 2018. The Committee notes it is conducting a related investigation into the use of social media by Russian-government affiliated entities.
[247] (U) The Fusion Center model is a partnership between DHS and state, local, tribal, and territorial entities. They serve as a focal point for "the receipt, analysis, gathering, and sharing of threat-related information."
[248] (U) CTIIC Cyber Threat Intelligence Summary/Cyber Threats in Focus, Malicious Cyber Activity on Election-Related Computer Networks Last Spring Possibly Linked to Russia, October 7, 2016; DHS, IIR 4 019 0147 16, September 28, 2016.
[249] (U) *Ibid.*
[250] (U) *Ibid.*

[redacted]

2. (U) Cyber Activity in State 4

(U[redacted]) State 4 officials, DHS, and FBI in the spring and summer of 2016, struggled to understand who was responsible for two rounds of cyber activity related to election infrastructure. Eventually, one set of cyber activity was attributed to Russia and one was not.

(U[redacted]) First, in April of 2016, a cyber actor successfully targeted State 4 with a phishing scam. After a county employee opened an infected email attachment, the cyber actor stole credentials, which were later posted online.[251] Those stolen credentials were used in June 2016 to penetrate State 4's voter registration database.[252] A CTIIC product reported the incident as follows: "An unknown actor viewed a statewide voter registration database after obtaining a state employee's credentials through phishing and keystroke logging malware, according to a private-sector DHS partner claiming secondhand access. The actor used the credentials to access the database and was in a position to modify county, but not statewide, data."[253]

(U[redacted]) DHS analysis of forensic data provided by a private sector partner discovered malware on the system, and State 4 shut down the voter registration system for about eight days to contain the attack.[254] State 4 officials later told the Committee that that while the cyber actor was able to successfully log in to a workstation connected to election related infrastructure, additional credentials would have been needed for the cyber actor to access the voter registration database on that system.[255]

(U) At first, FBI told State 4 officials that the attack may have originated from Russia, but the ties to the Russian government were unclear. "The Bureau described the threat as 'credible' and significant, a spokesman for State 4 Secretary of State said."[256] State 4 officials also told press that the hacker had used a server in Russia, but that the FBI could not confirm the

---

[251] (U) [redacted]

[252] (U) SSCI interview with DHS and CTIIC, February 27, 2018, p. 38.

[253] [redacted] Cyber Threat Intelligence Integration Center (CTIIC), Compromised State Election Networks, November 2, 2016, p. 1.

[254] (U[redacted]) DHS IIR 4 005 0829 16, *A* [redacted] *U.S. State Government's Election System Targeted by Malicious Activity*, September 9, 2016; Memorandum for the Record, SSCI Staff, Conference Call with [State 4], December 1, 2017.

[255] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 4], December 1, 2017.

[256] (U) [redacted]

attack was tied to the Russian government.[257] DHS and FBI later assessed it to be criminal activity, with no definitive tie to the Russian government.[258]

[redacted] Subsequently, Russian actors engaged in the same scanning activity as seen in other states, but directed at a domain affiliated with a public library.[259] Officials saw no effective penetration of the system. DHS has low confidence that this cyber activity is attributable to the Russian intelligence services because the target was unusual and not directly involved in elections.[260] [redacted]

V. (U) RUSSIAN INTENTIONS

(U) Russian intentions regarding U.S. election infrastructure remain unclear. Russia might have intended to exploit vulnerabilities in election infrastructure during the 2016 elections and, for unknown reasons, decided not to execute those options. Alternatively, Russia might have sought to gather information in the conduct of traditional espionage activities. Lastly, Russia might have used its activity in 2016 to catalog options or clandestine actions, holding them for use at a later date. Based on what the IC knows about Russia's operating procedures and intentions more broadly, the IC assesses that Russia's activities against U.S. election infrastructure likely sought to further their overarching goal: undermining the integrity of elections and American confidence in democracy.

- **(U)** Former-Homeland Security Adviser Lisa Monaco told the Committee that "[t]here was agreement [in the IC] that one of the motives that Russia was trying to do with this active measures campaign was to sow distrust and discord and lack of confidence in the voting process and the democratic process."[262]

- [redacted] DHS representatives told the Committee that "[w]e see . . . Russians in particular obviously, gain access, learn about the environment, learn about what systems are interconnected, probing, the type of intelligence preparation of the environment that you would expect from an actor like the Russians. So certainly the context going forward

---

[redacted]

[258] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 40.

[259] **(U)** [redacted]

[260] [redacted] DHS/FBI Homeland Intelligence Brief, [redacted]

[261] **(U)** *Ibid.*

[262] **(U)** SSCI Transcript of the Interview with of Lisa Monaco, Former Homeland Security Advisor, August 10, 2017, p. 30.

is a concern of what they might have learned and how much more they know about the systems."[263]

- [redacted] Mr. McCabe told the Committee that it seemed to him like "classic Russian cyber espionage. . . . [They will] scrape up all the information and the experience they possibly can," and "they might not be effective the first time or the fifth time, but they are going to keep at it until they can come back and do it in an effective way."[264]

- [redacted] Mr. Daniel told the Committee:

> *While any one voting machine is fairly vulnerable, as has been demonstrated over and over again publicly, the ability to actually do an operation to change the outcome of an election on the scale you would need to, and do it surreptitiously, is incredibly difficult. A much more achievable goal would be to undermine confidence in the results of the electoral process, and that could be done much more effectively and easily. . . . A logical thing would be, if your goal is to undermine confidence in the U.S. electoral system—which the Russians have a long goal of wanting to put themselves on the same moral plane as the United States . . . one way would be to cause chaos on election day. How could you start to do that? Mess with the voter registration databases.*[265]

- [redacted] Ms. Monaco further echoed that concern:

> *Well, one of the things I was worried about—and I wasn't alone in this—is kind of worst-case scenarios, which would be things like the voter registration databases. So if you're a state and local entity and your voter registration database is housed in the secretary of state's office and it is not encrypted and it's not backed up, and it says Lisa Monaco lives at Smith Street and I show up at my [polling place] and they say 'Well we don't have Ms. Monaco at Smith Street, we have her at Green Street,' now there's difficulty in my voting. And if that were to happen on a large scale, I was worried about confusion at polling places, lack of confidence in the voting system, anger at a large scale in some areas, confusion, distrust. So there was a whole sliding scale of*

---

[263] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 15.
[264] **(U)** DTS 2018-2152, SSCI Transcript of the Interview with Andrew McCabe, Former Deputy Director of the FBI, February 14, 2018, pp. 224-225.
[265] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, pp. 27, 34.

horribles just when you're talking about voter registration databases.[266]

- [redacted]

(U) Chaos on Election Day: Three Scenarios

[redacted] Mr. Daniel said that in the early fall of 2016, a policy working group was looking at three scenarios:

> *One was, could the Russians do something to the voter registration databases that could cause problems on Election Day? An example of that would be, could you go in and flip the digits in everybody's address, so that when they show up with their photo ID it doesn't match what's in the poll book? It doesn't actually prevent people from voting. In most cases you'll still get a provisional ballot, but if this is happening in a whole bunch of precincts for just about everybody showing up, it gives the impression that there's chaos.*[268]
>
> *A second one was to do a variant of the penetrating voting machines, except this time what you do is you do a nice video of somebody conducting a hack on a voting machine and showing how you could do that hack and showing them changing a voting outcome, and then you post that on YouTube and you claim you've done this 100,000 times across the United States, even though you haven't actually done it at all.*[269]
>
> *Then the third scenario that we looked at was conducting a denial of service attack on the Associated Press on Election Day, because pretty much everybody, all those nice maps that everybody puts up on all the different news services, is in fact actually based on Associated Press stringers at all the different precincts and locations. . . . It doesn't actually change anything, but it gives the impression that there's chaos.*[270]

---

[266] **(U)** SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, August 10, 2017, p. 28.

[267] [redacted]

[268] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, p. 33.

[269] **(U)** *Ibid.*, pp. 34-35.

[270] **(U)** *Ibid.*, p. 35.

VI. (U) NO EVIDENCE OF CHANGED VOTES OR MANIPULATED VOTE TALLIES

(U) In its review, the Committee has seen no indications that votes were changed, vote-tallying systems were manipulated, or that any voter registration data was altered or deleted, although the Committee and IC's insight is limited. Poll workers and voting monitors did not report widespread suspicious activity surrounding the 2016 election. DHS Assistant Secretary Jeanette Manfra said in the Committee's open hearing in June 2017 that "I want to reiterate that we do have confidence in the overall integrity of our electoral system because our voting infrastructure is fundamentally resilient." Further, all three witnesses in that hearing—Ms. Manfra, Dr. Liles, and FBI Assistant Director for Counterintelligence Bill Priestap—agreed that they had no evidence that votes themselves were changed in any way in the 2016 election.[271]

- **(U)** Dr. Liles said that DHS "assessed that multiple checks and redundancies in U.S. election infrastructure, including diversity of systems, non-internet connected voting machines, pre-election testing and processes for media, campaign and election officials to check, audit, and validate the results—all these made it likely that cyber manipulation of the U.S. election systems intended to change the outcome of the national election would be detected."[272] He later said "the level of effort and scale required to change the outcome of a national election would make it nearly impossible to avoid detection."[273]
- [redacted]
- **(U)** States did not report either an uptick in voters showing up at the polls and being unable to vote or a larger than normal quantity of provisional ballots.

(U) The Committee notes that nationwide elections are often won or lost in a small number of precincts. A sophisticated actor could target efforts at districts where margins are already small, and disenfranchising only a small percentage of voters could have a disproportionate impact on an election's outcome.

(U) Many state election officials emphasized their concern that press coverage of, and increased attention to, election security could create the very impression the Russians were seeking to foster, namely undermining voters' confidence in election integrity. Several insisted that whenever any official speaks publicly on this issue, they should state clearly the difference between a "scan" and a "hack," and a few even went as far as to suggest that U.S. officials stop

---

[271] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017.
[272] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 13.
[273] **(U)** *Ibid.*, p. 47.

talking about the issue altogether. One state official said, "We need to walk a fine line between being forthcoming to the public and protecting voter confidence."[274]

(U) Mr. Brennan described a similar concern in IC and policy discussions:

> *We know that the Russians had already touched some of the electoral systems, and we know that they have capable cyber capabilities. So there was a real dilemma, even a conundrum, in terms of what do you do that's going to try to stave off worse action on the part of the Russians, and what do you do that is going to . . . [give] the Russians what they were seeking, which was to really raise the specter that the election was not going to be fair and unaffected.*[275]

(U) Most state representatives interviewed by the Committee were confident that they met the threat effectively in 2016 and believed that they would continue to defeat threats in 2018 and 2020. Many had interpreted the events of 2016 as a success story: firewalls deflected the hostile activity, as they were supposed to, so the threat was not an issue. One state official told the Committee, "I'm quite confident our state security systems are pretty sound."[276] Another state official stated, "We felt good [in 2016]," and that due to additional security upgrades, "we feel even better today."[277]

(U) However, as of 2018, some states were still grappling with the severity of the threat. One official highlighted the stark contrast they experienced, when, at one moment, they thought elections were secure, but then suddenly were hearing about the threat.[278] The official went on to conclude, "I don't think any of us expected to be hacked by a foreign government."[279] Another official, paraphrasing a former governor, said, "If a nation-state is on the other side, it's not a fair fight. You have to phone a friend."[280]

(U) In the month before Election Day, DHS and other policymakers were planning for the worst-case scenario of efforts to disrupt the vote itself. Federal, state, and local governments created incident response plans to react to possible confusion at the polling places. Mr. Daniel said of the effort: "We're most concerned about the Russians, but obviously we are also concerned about the possibility for just plain old hacktivism on Election Day. . . . The incident response plan is actually designed . . . to help us [plan for] what is the federal government going to do if bad things start to happen on Election Day?"

[redacted] Mr. Daniel added that this was the first opportunity to exercise the process established under Presidential Policy Directive-41. "We asked the various agencies with lead

---

[274] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[275] **(U)** SSCI Transcript of the Interview with John Brennan, Former Director, CIA, held on Friday, June 23, 2017, p. 54.
[276] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017.
[277] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[278] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 20], November 17, 2017.
[279] **(U)** *Ibid.*
[280] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.

responsibility, all right, give us your Election Day plan." That led to the creation of an Election Day playbook; steps included enhanced watch floor procedures, connectivity between FBI field offices and FBI and DHS, and an "escalation path" if "we needed to get to Lisa [Monaco] or Susan [Rice] in a hurry" on Election Day.[281]

VII. (U) SECURITY OF VOTING MACHINES

(U) The Committee review of Russian activity in 2016 highlighted potential vulnerabilities in many voting machines, with previous studies by security researchers taking on new urgency and receiving new scrutiny. Although researchers have repeatedly demonstrated it is possible to exploit vulnerabilities in electronic voting machines to alter votes,[282] some election officials dispute whether such attacks would be feasible in the context of an actual election.

- **(U)** Dr. Alex Halderman, Professor of Computer Science at the University of Michigan, testified before the Committee in June 2017 that "our highly computerized election infrastructure is vulnerable to sabotage and even to cyber attacks that could change votes."[283] Dr. Halderman concluded, "Voting machines are not as distant from the internet as they may seem."[284]

- **(U)** When State 7 decommissioned its Direct-Recording Electronic (DRE) voting machines in 2017, the IT director led an exercise in attempting to break into a few of the machines using the access a "normal" voter would have in using the machines.[285] The results were alarming: the programmed password on some of the machines was ABC123, and the testers were able to flip the machines to supervisor mode, disable them, and "do enough damage to call the results into question."[286] The IT director shared the results with State 21 and State 24, which were using similiar machines.[287]

- **(U)** In 2017, DEFCON[288] researchers were able to find and exploit vulnerabilities in five different electronic voting machines.[289] The WinVote machines, those recently decertified by State 7, were most easily manipulated. One attendee said, "It just took us a couple of hours on Google to find passwords that let us unlock the administrative

---

[281] **(U)** *Ibid.*, p. 82.
[282] **(U)** *See also, infra*, "Direct-Recording Electronic (DRE) Voting Machine Vulnerabilities."
[283] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 117.
[284] **(U)** *Ibid.*, p. 110.
[285] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.
[286] **(U)** *Ibid.* The machines used were WinVote voting machines.
[287] **(U)** *Ibid.*
[288] **(U)** DEFCON is an annual hacker conference held in Las Vegas, Nevada. In July 2017, at DEFCON 25, the conference featured a Voting Machine Hacking Village ("Voting Village") which acquired and made available to conference participants over 25 pieces of election equipment, including voting machines and electronic poll books, for generally unrestricted examination for vulnerabilities.
[289] **(U)** Matt Blaze, et. al., *DEFCON 25: Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, September 2017, https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20report.pdf, pp. 8-13.

functions on this machine."[290] A researcher was able to hack into the WinVote over WiFi within minutes using a vulnerability from 2003.[291] Once he had administrator-level access, he could change votes in the database. Researchers also discovered available USB ports in the machine that would allow a hacker to run software on the machine.[292] One said "with physical access to back [sic] of the machine for 15 seconds, an attacker can do anything."[293] Hackers were less successful with other types of machines, although each had recorded vulnerabilities.[294]

- **(U)** The 2018 DEFCON report found similar vulnerabilities, in particular when hackers had physical access to the machines. For example, hackers exploited an old vulnerability on one machine, using either a removable device purchasable on eBay or remote access, to modify vote counts.[295]

- **(U/[redacted])** DHS briefed the Committee in August 2018 that these results were in part because the hackers had extended physical access to the machines, which is not realistic for a true election system. Undersecretary Krebs also disagreed with reporting that a 17-year-old hacker had accessed voter tallies.[296] Some election experts have called into question the DEFCON results for similar reasons and pointed out that any fraud requiring physical access would be, by necessity, small scale, unless a government were to deploy agents across thousands of localities.

- **(U)** ES&S Voting Systems disclosed that some of its equipment had a key security vulnerability. ES&S installed remote access software on machines it sold in the mid-2000s, which allowed the company to provide IT support more easily, but also created potential remote access into the machines. When pressed by Senator Ron Wyden of Oregon, the company admitted that around 300 voting jurisdictions had the software. ES&S says the software was not installed after 2007, and it was only installed on election-management systems, not voting machines.[297] More than 50 percent of voters vote on ES&S equipment, and 41 states use its products.

---

[290] **(U)** Elizabeth Wise, "Hackers at DefCon Conference Exploit Vulnerabilities in Voting Machines," *USA Today*, July 30, 2017, https://www.usatoday.com/story/tech/2017/07/30/hackers-defcon-conference-exploit-vulnerabilities-voting-machines/523639001/.
[291] **(U)** Matt Blaze, et. al., *DEFCON 25: Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, September 2017, https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20report.pdf, p. 4.
[292] **(U)** *Ibid.*, p. 9.
[293] **(U)** *Ibid.*
[294] **(U)** *Ibid.*, pp. 8-13.
[295] **(U)** Robert McMillian and Dustin Volz, "Voting Machine Used in Half of U.S. Is Vulnerable to Attack, Report Finds," *Wall Street Journal*, September 27, 2018. The machine referenced is the ES&S Model 650, which ES&S stopped making in 2008 but is still available for sale.
[296] **(U)** DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018
[297] **(U)** Hacks, Security Gaps And Oligarchs: The Business of Voting Comes Under Scrutiny. Miles Parks, NPR, September 21, 2018.

(U) Advocates of electronic voting point out the flaws in paper ballots, like the potential for the introduction of fraudulent ballots or invalidated votes due to stains or extra marks. The Committee believes that any election system should be protected end-to-end, including against fraud.

(U) Direct-Recording Electronic (DRE) Voting Machine Vulnerabilities

(U) While best practices dictate that electronic voting machines not be connected to the internet, some machines are internet-enabled. In addition, each machine has to be programmed before Election Day, a procedure often done either by connecting the machine to a local network to download software or by using removable media, such as a thumb drive. These functions are often carried out by local officials or contractors. If the computers responsible for writing and distributing the program are compromised, so too could all voting machines receiving a compromised update. Further, machines can be programmed to show one result to the voter while recording a different result in the tabulation. Without a paper backup, a "recount" would use the same faulty software to re-tabulate the same results, because the primary records of the vote are stored in computer memory.[298]

(U) Dr. Halderman said in his June 2017 testimony before SSCI:

> *I know America's voting machines are vulnerable because my colleagues and I have hacked them repeatedly as part of a decade of research studying the technology that operates elections and learning how to make it stronger. We've created attacks that can spread from machine to machine, like a computer virus, and silently change election outcomes. We've studied touchscreen and optical scan systems, and in every single case we found ways for attackers to sabotage machines and to steal votes. These capabilities are certainly within reach for America's enemies.*
>
> *Ten years ago, I was part of the first academic team to conduct a comprehensive security analysis of a DRE voting machine. We examined what was at the time the most widely used touch-screen DRE in the country and spent several months probing it for vulnerabilities. What we found was disturbing: we could reprogram the machine to invisibly cause any candidate to win.*[299]

---

[298] **(U)** "Some DREs also produce a printed record of the vote and show it briefly to the voter, using a mechanism called a voter-verifiable paper audit trail, or VVPAT. While VVPAT records provide a physical record of the vote that is a valuable safeguard against cyberattacks, research has shown that VVPAT records are difficult to accurately audit and that voters often fail to notice if the printed record doesn't match their votes. For these reasons, most election security experts favor optical scan paper ballots." Written Statement by J. Alex Halderman, June 21, 2017, citing S. Goggin and M. Byrne, "An Examination of the Auditability of Voter Verified Paper Audit Trail (VVPAT) Ballots," *Proceedings of the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop*, August 2007; B. Campbell and M. Byrne, "Now do Voters Notice Review Screen Anomalies?" *Proceedings of the 2009 USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop*, August 2009.

[299] **(U)** The machine was the Diebold AccuVote TS, which was still used statewide in at least one state as of 2017.

> *Cybersecurity experts have studied a wide range of U.S. voting machines—including both DREs and optical scanners—and in* every single case, *they've found severe vulnerabilities that would allow attackers to sabotage machines and to alter votes. That's why there is overwhelming consensus in the cybersecurity and election integrity research communities that our elections are at risk.*[300]

(U) In speaking with the Committee, federal government officials revealed concerns about the security of voting machines and related infrastructure. Former Assistant Attorney General for National Security John Carlin told the Committee:

> *"I'm very concerned about . . . our actual voting apparatus, and the attendant structures around it, and the cooperation between some states and the federal government."*[301] *Mr. Carlin further stated, "We've literally seen it already, so shame on us if we can't fix it heading into the next election cycles. And it's the assessment of every key intel professional, which I share, that Russia's going to do it again because they think this was successful. So we're in a bit of a race against time heading up to the two-year election. Some of the election machinery that's in place should not be."*[302]

(U) Mr. McCabe echoed these concerns, and noted that, in the last months before the election, FBI identified holes in the security of election machines, saying "there's some potential there."[303]

(U) As of November 2016, five states were using exclusively DRE voting machines with no paper trail, according to open source information.[304] An additional nine states used at least some DRE voting machines with no paper trail.[305]

- **(U)** State 20 has 21-year-old DRE machines. While the state is in the process of replacing its entire voting system, including these machines, State 20 is aiming to have the updates ready for the 2020 elections.

- **(U)** In State 21, 50 of 67 counties as of November 2017 used DRE voting machines.[306]

---

[300] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, pp. 116-117.
[301] **(U)** SSCI Transcript of the Interview with John Carlin, Former Assistant Attorney General for National Security, held on Monday, September 25, 2017, p. 86.
[302] **(U)** *Ibid.*, pp. 86-87.
[303] **(U)** DTS 2018-2152, SSCI Interview with Andrew McCabe, Former Deputy Director of the FBI, February 14, 2018, p. 221.
[304] **(U)** BallotPedia, *Voting Methods and Equipment By State*, https://ballotpedia.org/Voting_methods_and_equipment_by_state.
[305] **(U)** *Ibid.*
[306] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 21], November 17, 2017.

- (U) State 5 used paper-backed voting in only about half its machines and DRE voting machines without paper backup in the other half.[307]

- (U) Some states are moving to a hybrid model—an electronic voting machine with a paper backup, often in the form of a receipt that prints after the voter submits their vote. For example, State 12 uses some DREs, but all equipment is required to have a paper trail, and the paper ballot is the ballot of record.[308] State 12 also conducts a mandatory state-wide audit.[309] Similarly, State 13 uses some paper-based and some electronic machines, but all are required to have a paper trail.[310]

(U) The number of vendors selling voting machines is shrinking, raising concerns about a vulnerable supply chain. A hostile actor could compromise one or two manufacturers of components and have an outsized effect on the security of the overall system.

- [redacted] "My job," said Ms. Monaco when asked whether she was worried about voting machines themselves getting hacked, "was to worry about every parade of horribles. So I cannot tell you that that did not cross my mind. We were worried about who, how many makers. We were worried about the supply chain for the voting machines, who were the makers? . . . Turns out I think it's just Diebold—and have we given them a defensive briefing? So to answer your question, we were worried about it all."[311]

- [redacted] Mr. McCabe pointed out that a small number of companies have "90%" of the market for voting machines in the U.S. Before the 2016 election, [redacted] briefed a few of the companies on vulnerabilities,[312] but a more comprehensive campaign to educate vendors and their customers is warranted.

(U) Voluntary Voting System Guidelines

(U) Part of the voting reform implemented under The Help America Vote Act of 2002 was a requirement that the Election Assistance Commission create a set of specifications and requirements against which voting systems can be tested, called the Voluntary Voting System Guidelines (VVSG). The EAC adopted the first VVSG in December 2005. The EAC then tasked the Technical Guidelines Development Committee, chaired by the National Institute of Standards and Technology (NIST) and including members from NASED, with updating the guidelines. In March 2015, the EAC approved VVSG 1.1; in January 2016, the EAC adopted

---

[307] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 5], December 1, 2017.
[308] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 12], December 1, 2017.
[309] (U) *Ibid.*
[310] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.
[311] (U) SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, p. 31.
[312] (U) SSCI Transcript of the Interview with Andy McCabe, Deputy Director of the FBI, held on Wednesday, February 14, 2018, pp. 220-221.

an implementation plan requiring that all new voting systems be tested against the VVSG 1.1 beginning in July 2017. VVSG 1.1 has since been succeeded by version 2.0, which was released for a 90-day public comment period on February 15, 2019. The EAC will compile the feedback for Commissioners to review shortly thereafter.[313] VVSG 2.0 includes the following minimum security guidelines:

- **(U)** An error or fault in the voting system software or hardware cannot cause an undetectable change in election results. (9.1)
- **(U)** The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities. (9.2)
- **(U)** Voting system records are resilient in the presence of intentional forms of tampering and accidental errors. (9.3)
- **(U)** The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. (11.3)
- **(U)** The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records. (13.1)
- **(U)** The voting system limits its attack surface by reducing unnecessary code, data paths, physical ports, and by using other technical controls. (14.2)
- **(U)** The voting system employs mechanisms to protect against malware. (15.3)
- **(U)** A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice. (15.4)

(U) As of March 2018, 35 states required that their machines be certified by EAC, but compliance with the VVSG standards is not mandatory. Secretary Nielsen testified before the Committee that the United States should "seek for all states" to use the VVSG standards.[314]

---

[313] **(U)** *EAC Commissioners Unanimously Vote to Publish VVSG 2.0 Principles and Guidelines for Public Comment*: https://www.eac.gov/news/2019/02/15/eac-commissioners-unanimously-vote-to-publish-vvsg-20-principles-and-guidelines-for-public-comment/; February 15, 2019

[314] **(U)** SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p. 47.

VIII. (U) THE ROLE OF DHS AND INTERACTIONS WITH THE STATES

(U) The federal government's actions to address election security threats evolved significantly from the summer of 2016 through the summer of 2018. Contemporaneous with the Russian attacks, DHS and FBI were initially treating the situation as they would a typical notification of a cyber incident to a non-governmental victim. By the fall of 2016, however, DHS was attempting to do more extensive outreach to the states. Then in the fall of 2017, DHS undertook an effort to provide a menu of cyber support options to the states.

A. (U) DHS's Evolution

[redacted] For DHS and other agencies and departments tasked with intelligence collection or formulating policy options through the interagency process, the full scope of the threat began to emerge in the summer of 2016. Secretary Johnson told the Committee that "I know I had significant concerns by [summer of 2016] about doing all we could to ensure the cybersecurity of our election systems."[315] Mr. Daniel said in his interview that by the end of July, the interagency was focused on better protecting electoral infrastructure as part of a "DHS and FBI-led domestic effort."[316]

[redacted] Policymakers quickly realized, however, that DHS was poorly positioned to provide the kind of support states needed. Mr. Daniel said that interagency discussions about the threat "start[ed] a process of us actually realizing that, frankly, we don't actually have very much in the way of capability that we can directly offer the states"—a fact that the states themselves would later echo.[317]

- [redacted] Ms. Monaco said that DHS initially found a "pretty alarming variance in the number of voting registration databases and lack of encryption and lack of backup for all of these things."[318] Ms. Monaco added that "[i]n light of what we were seeing, in light of the intelligence we were getting briefed on, this was a very specific direction and decision to say we need to really accelerate this, put a significant push on resources and engagement at the senior-most levels."[319]

- [redacted] Mr. Daniel and the working group identified DHS's cyber teams as possible assistance to the states. "DHS had teams that could go and provide that support to the private sector. We've been doing that. That's a program that existed for years for critical

---

[315] (U) SSCI Transcript of the Interview with Jeh Johnson, Former Secretary of Homeland Security, held on Monday, June 12, 2017, p. 10.
[316] (U) SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 28.
[317] (U) *Ibid.*, p. 38.
[318] (U) SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, SSCI interview of Lisa Monaco, August 10, 2017, p. 19.
[319] (U) *Ibid.*, p. 21.

infrastructure companies. And we realized that we could repurpose [some of those teams], but we don't have that many of them . . . four or five. It was not very many."[320]

(U) DHS attempted a nuanced outreach to the states on the threat. Ms. Monaco highlighted a delicate balancing act with the interactions with states:

> *I know we tried very hard to strike a balance between engaging state and local officials and federal officials in the importance of raising cyber defenses and raising cybersecurity . . . and not sowing distrust in the system, both because, one, we believed it to be true that the system is in fact quite resilient because of what I mentioned earlier, which is the diffuse nature; and because we did not want to, as we described it, do the Russians' work for them by sowing panic about the vulnerability of the election.*[321]

(U) In an August 15, 2016, conference call with state election officials, then-Secretary Johnson told states, "we're in a sort of a heightened state of alertness; it behooves everyone to do everything you can for your own cybersecurity leading up to the election." He also said that there was "no specific or credible threat known around the election system itself. I do not recall—I don't think, but I do not recall, that we knew about [State 4] and Illinois at that point."[322] The Committee notes that this call was two months after State 4's system was breached, and more than a month after Illinois was breached and the state shut down its systems to contain the problem. During this call, Secretary Johnson also broached the idea of designating election systems as critical infrastructure.

(U) A number of state officials reacted negatively to the call. Secretary Johnson said he was "surprised/disappointed that there was a certain level of pushback from at least those who spoke up. . . . The pushback was: This is our—I'm paraphrasing here: This is our responsibility and there should not be a federal takeover of the election system."[323]

- **(U)** The call "does not go incredibly well," said Mr. Daniel. "I was not on the call, no, but all of the reporting back and then all of the subsequent media reporting that is leaked about the call shows that it did not go well." Mr. Daniel continued: "I was actually quite surprised . . . in my head, there is this: yes, we have this extremely partisan election going on in the background; but the Russians are trying to mess with our election. To me, that's a national security issue that's not dependent on party or anything else."[324]

---

[320] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 41.
[321] **(U)** SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, p. 29.
[322] **(U)** SSCI Transcript of the Interview with Jeh Johnson, Former Secretary of Homeland Security, held on Monday, June 12, 2017, p. 13.
[323] **(U)** *Ibid.*, pp. 13-14.
[324] **(U)** *Ibid.*, p. 48.

- (U) Ms. Monaco also related how DHS received significant push back from the states and decided to "focus our efforts on really pushing states to voluntarily accept the assistance that DHS was trying to provide."[325]

- (U) States also reported that the call did not go well. Several states told the Committee that the idea of a critical infrastructure designation surprised them and came without context of a particular threat. Some state officials also did not understand what a critical infrastructure designation meant, in practical terms, and whether it would give the federal government the power to run elections. DHS also did not anticipate a certain level of suspicion from the states toward the federal government. As a State 17 official told the Committee, "when someone says 'we're from the government and we're here to help,' it's generally not a good thing."[326]

(U) Critical Infrastructure Designation

(U) One of the most controversial elements of the relationship between DHS and the states was the decision to designate election systems as critical infrastructure. Most state officials relayed that they were surprised by the designation and did not understand what it meant; many also felt DHS was not open to input from the states on whether such a designation was beneficial.

(U) Secretary Johnson remembers the first time he aired the possibility of a designation was on August 3, 2016. He went to a reporters' breakfast sponsored by the Christian Science Monitor and publicly "floated the idea of designating election infrastructure as critical infrastructure."[327] Then, on August 15, 2016, Secretary Johnson had a conference call with election officials from all 50 states. "I explained the nature of what it means to be designated critical infrastructure. It's not a mandatory set of [regulations], it's not a federal takeover, it's not binding operational directives. And here are the advantages: priority in terms of our services and the benefit of the protection of the international cyber norm."[328] Secretary Johnson continued: "I stressed at the time that this is all voluntary and it prioritizes assistance if they seek it."[329]

(U) Some states were vocal in objecting to the idea. In evaluating the states' response, DHS came to the conclusion that it should put the designation on hold, deciding it would earn more state trust and cooperation if it held off on the designation as critical infrastructure and perhaps sought more buy-in from the states at a later date.[330]

---

[325] **(U)** SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, SSCI interview of Lisa Monaco, August 10, 2017, p. 25.
[326] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with State 17, January 25, 2018.
[327] **(U)** SSCI Transcript of the Interview with Jeh Johnson, Former Secretary of Homeland Security, held on Monday, June 12, 2017, p. 10.
[328] **(U)** *Ibid.*, p. 14. For additional information on the definition of critical infrastructure in a cybersecurity context, *see* Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013.
[329] **(U)** SSCI Transcript of the Open Hearing on Election Security, March 21, 2018, p. 34.
[330] **(U)** *Ibid.*, p. 115.

(U) After the election, Secretary Johnson decided the time had come to make the designation. He held a follow-up call with NASS on the critical infrastructure designation in January 2017: "I didn't tell them I'm doing this the next day, but I told them I was close to making a decision. I didn't hear anything further [along the lines of additional, articulated objections], so the same day we went public with the [unclassified] version of the report,[331] I also made the designation."[332]

(U) Mr. Daniel summed up the rationale for proceeding this way: "I do believe that we should think of the electoral infrastructure as critical infrastructure, and to me it's just as critical for democracy as communications, electricity, water. If that doesn't function, then your democracy doesn't function. . . . To me that is the definition of 'critical.'"[333]

(U) In interviews with the Committee in late 2017 and early 2018, several states were supportive of the designation and saw the benefits of, for example, the creation of the Government Coordinating Council. Others were lukewarm, saying they had seen limited benefits for all the consternation officials said it had caused. Still others remained suspicious that the designation is a first step toward a federal takeover of elections.

B. (U) The View From the States

(U) For most states, the story of Russian attempts to hack state infrastructure was one of confusion and a lack of information. It began with what states interpreted as an insignificant event: an FBI FLASH notification on August 18, 2016, [redacted][334] Then, in mid-October, the MS-ISAC reached out to state IT directors with an additional alert about specific IP addresses scanning websites.[335] At no time did MS-ISAC or DHS identify the IP addresses as associated with a nation-state actor. Given the lack of context, state staff who received the notification did not ascribe any additional urgency to the warning; to them, it was a few more suspect IP addresses among the thousands that were constantly pinging state systems. Very few state IT directors informed state election officials about the alert.

---

[331] (U) Secretary Johnson was referring to the declassified version of the Intelligence Community Assessment, *Assessing Russian Activities and Intentions in Recent U.S. Elections*, January 6, 2017.
[332] (U) *Ibid.*, p. 46.
[333] (U) SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 98.
[334] (U) FBI FLASH, Alert Number T-LD1004-TT, TLP-AMBER, [redacted]
[335] (U) FBI FLASH, Alert Number T-LD1005-TT, TLP-AMBER, [redacted]; DHS/FBI JAR-16-20223, *Threats to Federal, State, and Local Government Systems*, October 14, 2016.

- **(U)** State 11 had a meeting with DHS officials, including the regional DHS cyber advisor, in August 2016, but according to State 11 officials, DHS did not mention any specific threat against election systems from a nation-state actor.[336]

- **(U)** State 13 reported that DHS contacted an affected county at one point, but never contacted the state-level officials.[337]

- **(U)** When they saw an IP address identified in the alerts had scanned their systems, State 6 and State 16 sent their logs to the MS-ISAC for analysis.[338] State 16 said it never received a response.[339]

(U) DHS, conversely, saw its efforts as far more extensive and effective. Ms. Manfra testified to SSCI that DHS "held a conference call where all 50 secretaries of state or an election director if the secretary of state didn't have that responsibility [participated], in August, in September, and again in October [of 2016], both high-level engagement and network defense products [sic]."[340] Mr. Daniel reported that "by the time Election Day rolls around, all but one state has taken us up on the offer to at least do scanning [,] so I want to give people credit for not necessarily sticking to initial partisan reactions and . . . taking steps to protect their electoral infrastructure."[341]

(U) States reported to the Committee that Election Day went off smoothly. For most state election officials, concerns about a possible threat against election systems dropped off the radar until the summer or fall of 2017. Many state election officials reported hearing for the first time that Russian actors were responsible for scanning election infrastructure in an estimated 21 states from the press or from the Committee's open hearing on June 21, 2017. During that hearing, in response to a question from Vice Chairman Warner inquiring whether all affected states were aware they were attacked, Ms. Manfra responded that "[a]ll of the system owners within those states are aware of the targeting, yes, sir."[342] However, when pressed as to whether election officials in each state were aware, the answer was less clear.[343]

- **(U)** In that hearing, Dr. Liles said DHS had "worked hand-in-hand with the state and local partners to share threat information related to their networks."[344]

---

[336] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 11], December 8, 2017.
[337] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.
[338] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017; Memorandum for the Record, SSCI Staff, Conference Call with [State 16], December 1, 2017.
[339] **(U)** *Ibid.* State 6 did not indicate whether they received feedback from DHS.
[340] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, June 21, 2017, p. 74.
[341] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 49.
[342] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 28.
[343] **(U)** *Ibid.*, pp. 62-63.
[344] **(U)** *Ibid.*, p. 12.

- (U) Ms. Manfra said, "The owners of the systems within those 21 states have been notified." Senator King then asked, "How about the election officials in those states?" Ms. Manfra responded, "We are working to ensure that election officials as well understand. I'll have to get back to you on whether all 21 states ....[crosstalk]."[345]

- (U) Given Ms. Manfra's testimony and the fact that some election officials did not get a notification directly to their offices, election officials in many states assumed they were not one of the 21; some even issued press releases to that effect.[346]

(U) The disconnect between DHS and state election officials became clear during Committee interactions with the states throughout 2017. In many cases, DHS had notified state officials responsible for network security, but not election officials, of the threat. Further, the IT professionals contacted did not have the context to know that this threat was any different than any other scanning or hacking attempt, and they had not thought it necessary to elevate the warning to election officials.

(U) After the hearing, and in part to respond to confusion in the states, DHS held a conference call with representatives from 50 states in September 2017. In that call, DHS said they would contact affected states directly. State 8 state election officials noted that the call became "somewhat antagonistic."[347] State 17 officials reported that the phone call "just showed how little DHS knew about elections."[348] Several officials argued that all 50 states should be notified of who had been hacked. DHS followed up with one-to-one phone calls to states over the next several days.

- (U) Officials from some states reported being shocked that they were in fact one of the states, and further surprised that their states had supposedly been notified.

- (U) Most state officials found the conference calls lacking in information and were left wondering exactly what the threat might be. Several states said the DHS representatives could not answer any specific questions effectively.

(U) Following this series of difficult engagements, DHS set about trying to build relationships with the states, but it faced a significant trust deficit. Early follow-up interactions between state election officials and DHS were rocky. States reported that DHS seemed to have little to no familiarity with elections. For example, State 6 said that the DHS representatives they were assigned seemed to know nothing about State 6, and, when pressed, they admitted they were "just reading the spreadsheet in front of [them]."[349] State 8 reported that "we are spending

---

[345] (U) *Ibid.*, pp. 62-63.
[346] (U) State 8 said they put out a press release because DHS had said publicly that they had notified the 21 states, and "if you were one of the 21, you would know."
[347] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[348] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 17], January 25, 2018.
[349] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017.

a ton of time educating outside groups on how elections are run."[350] State 3 officials said, "DHS didn't recognize that securing an election process is not the same as securing a power grid."[351]

(U) By early 2018, State officials gave DHS credit for making significant progress over the next six months. States began to sign up for many of the resources that DHS had to offer, and DHS hosted the first meeting of the Government Coordinating Council required under the critical infrastructure designation. Those interactions often increased trust and communication between the federal and state entities. For example, DHS has identified a list of contacts to notify if they see a threat; that list includes both IT officials and election officials. State 9 described it as "quite a turnaround for DHS," and further stated that the Secretaries of State had been disappointed with how slowly DHS got up to speed on election administration and how slowly the notifications happened, but DHS was "quick with the *mea culpas* and are getting much better." [352]

(U) Not all of the engagements were positive, however. State 13 in early December 2017 still reported continued frustration with DHS, indicating to the Committee that it had not seen much change in terms of outreach and constructive engagement. As of summer 2017, according to State 13, "the lack of urgency [at DHS] was beyond frustrating."[353]

C. (U) Taking Advantage of DHS Resources

(U) As DHS has pursued outreach to the states, more and more have opened their doors to DHS assistance. DHS told the Committee that its goal has been relationship building and:

> *In the partnerships with the states and secretaries of states, state election directors, and at the local level, we're trying to shift them to a culture of more information security management, where they can now account for the integrity of their system, or, if something did happen . . . they know the full extent of what happened on their system. . . . We're providing vulnerability assessments and trend analysis, in addition to connecting them to the threat intelligence that we can, in order to evolve their . . . cyber culture.* [354]

(U) DHS's assistance can be highly tailored to need, and falls into roughly two buckets: remote cyber hygiene scans, which provide up to weekly reports, and on-site risk and vulnerability assessments. DHS also offers a suite of other services, including phishing campaign assessments. All these efforts seek to provide the states with actionable information to improve cyber hygiene, but DHS has been keen to avoid what could be perceived by the states as

---

[350] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[351] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 3], December 8, 2017.
[352] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.
[353] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.
[354] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, pp. 54-55.

unfunded mandates.[355] Some states requesting more intensive services have also experienced significant delays before DHS could send a team to assist.

- **(U)** By October 2018, DHS said 35 states, 91 local jurisdictions, and eight election system vendors had signed up for remote persistent scans.[356] All the requests for these scans have been fulfilled. "They can be turned on basically within the week," according to DHS.[357]

- **(U)** DHS said that as of October 2018, it had completed 35 in-depth, on the ground vulnerability assessments: 21 states, 13 localities, and one election system vendor. These assessments are one week off-site remote scans followed by a second week on site.[358]

- **(U)** Two states who completed the in-depth assessments reported in late 2017 they had had a good experience. State 12 officials said the team was "extremely helpful and professional."[359] State 10 said the review was a good experience, although DHS was somewhat limited in what it could do.[360] For example, DHS did a phishing email test that showed the training for employees had worked.[361] DHS gave "good and actionable recommendations." Although DHS "didn't really understand election systems when they came," they learned a lot.[362]

- **(U)** As of November 2017, State 6 and State 9 requested an on-site scan, but those scans were on track to be delayed past the August 2018 primaries.[363] State 7 was expecting a four-to-six month delay.[364] State 8 signed up for a checkup in October 2017 and was due to get service the following February.[365] As of January 2018, State 17 also had requested an on-site scan.[366]

(U) In a sign of improving relations between the states and DHS, two states that had elections in 2017 attempted to include DHS in the process more extensively than in the past. In State 17, a two-person DHS team sat with election officials during the 2017 special election and monitored the networks. Even though "their presence was comforting," they "really didn't do much." State 17 signed DHS's normal MOU, but also added its own clause to underscore the state's independence: a formal sunset on DHS's access to state systems, one week after the

---

[355] **(U)** *Ibid.*, p. 60.
[356] **(U)** *Ibid.*, p. 57.
[357] **(U)** DHS phone call with SSCI: October 16, 2018.
[358] **(U)** *Ibid*
[359] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 12], December 1, 2017.
[360] **(U)** *Ibid.*
[361] **(U)** *Ibid.*
[362] **(U)** *Ibid.*
[363] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017; Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.
[364] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.
[365] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[366] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 17], January 25, 2018.

election. State 7 reported their experience with DHS during the 2017 statewide election was quite good. DHS sat with election officials all day, which meant State 7 could pass messages quickly to NCCIC.

(U) In March 2018, Congress appropriated $380 million in funding for election security improvements. The funding was distributed under the formula laid out in the Help American Vote Act (HAVA) and was intended to aid in replacing vulnerable voting machines and improving cybersecurity. As of July 2018, 13 states said they intended to use the funds to buy new voting machines, and 22 said they have "no plans to replace their machines before the election—including all five states that rely solely on paperless electronic voting devices," according to a survey by Politico.[367]

IX. (U) RECOMMENDATIONS

1. (U) Reinforce States' Primacy in Running Elections*

(U) States should remain firmly in the lead on running elections, and the federal government should ensure they receive the necessary resources and information.

2. (U) Build a Stronger Defense, Part I: Create Effective Deterrence

(U) The United States should communicate to adversaries that it will view an attack on its election infrastructure as a hostile act, and we will respond accordingly. The U.S. Government should not limit its response to cyber activity; rather, it should create a menu of potential responses that will send a clear message and create significant costs for the perpetrator.

[redacted] **Ideally, this principle of deterrence should be included in an overarching cyber doctrine for the U.S. Government.** That doctrine should clearly delineate cyberespionage, cybercrime, and cyber attacks. Further, a classified portion of the doctrine should establish what the U.S. Government believes to be its escalation ladder in the cyber realm—what tools does it have, what tools should it pursue, and what should the limits of cyber war be. The U.S. strategic approach tends to overmatch adversaries with superior technology, and policymakers should consider what steps the U.S. will need to take to outstrip the capabilities of Russia, China, Iran, North Korea, and other emerging hostile actors in the cyber domain.

(U) U.S. cyber doctrine should serve as the basis for a discussion with U.S. allies and others about new cyber norms. Just as the international community has established norms and treaties about the use of technologies and weapons systems, the U.S. should lead a conversation about cyber norms and the limits of cyber activity with allies and others.

*The Committee's recommendation to "reinforce states' primacy in running elections" should be understood in reference to states' responsibility for election security, and not as pertaining to broader election issues, such as campaign finance laws or voting rights laws.

[367] (U) States Slow to Prepare for Hacking Threats, Eric Geller, Politico, July 18, 2018.

3. **(U) Build a Stronger Defense, Part II: Improve Information Gathering and Sharing on Threats**

[redacted]

[redacted] **The U.S. government needs to build the cyber expertise and capacity of its domestic agencies, such as DHS and FBI, and reevaluate the current authorities that govern efforts to defend against foreign cyber threats.** NSA and CIA collection is, by law, directed outside the United States. [redacted]

[redacted] **The U.S. government should invest in capabilities for rapid attribution of cyber attacks, without sacrificing accuracy.** [redacted] However, the IC needs to improve its ability to provide timely and actionable warning. Timely and accurate attribution is not only important to defensive information sharing, but will also underpin a credible deterrence and response strategy.

(U) The federal government and state governments need to create clear channels of communication two ways—down from the federal government to the state and local level, and up from the state and local officials on the front lines to federal entities. In 2016, DHS and FBI did not provide enough information or context to election officials about the threat they were facing, but states and DHS have made significant progress in this area in the last two years. For example, Secretary of Homeland Security Nielsen testified to the Committee in March 2018 that "today I can say with confidence that we know whom to contact in every state to share threat information. That capability did not exist in 2016."[369]

(U) A key component of information sharing about elections is security clearances for appropriate officials at the state and local level. DHS and its partners can effectively strip classified information off of cyber indicators, which can then be passed to technical staff at the state level, but in order for those indicators to not get lost in the multitude of cyber threats those professionals see on a daily basis, senior officials at the state and local levels need to know the

---

[368] [redacted]

[369] (U) SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p. 16.

context surrounding the indicators. State officials need to know why a particular threat is of significant concern, and should be prioritized. That context could come from classified information, or states could come to understand that threat information DHS passes them is more serious than that received through other sources. DHS's goal is to obtain clearances for up to three officials per state.[370] As of August 2018, DHS had provided a clearance to 92 officials[371]; as of late 2017 all state election officials had received interim secret clearances or one-day read-ins for secret-level briefings.[372] DHS, along with ODNI and FBI, also hosted state and local election officials for a SECRET-level briefing on the sidelines of the biannual NASS and NASS-ED conferences in Washington, DC in February 2018. In March, Amy Cohen, Executive Director of NASS-ED testified in front of the Committee that, "It would be naïve to say that we received answers to all our questions, but the briefing was incredibly valuable and demonstrated how seriously DHS and others take their commitment to the elections community as well as to our concerns."[373] The Committee recommends DHS continue providing such briefings and improve the quality of information shared.

(U) Fundamental to meaningful information sharing, however, is that state officials understand what they are getting. New inductees to the world of classified information are often disappointed—they expected to see everything laid out in black and white, when intelligence is often very gray, with a pattern discernable only to those who know where to look and what conclusions to draw. Those sharing the intelligence should manage expectations—at the SECRET level, officials are likely to see limited context about conclusions, but not much more.

(U) Federal officials should work to declassify information, for the purpose of providing warning to appropriate state and local officials, to the greatest extent possible. If key pieces of context could be provided at a lower classification level while still protecting classified information, DHS and its partners should strive to do so.

4. (U) Build a Stronger Defense, Part III: Secure Election-Related Cyber Systems

(U) Despite the expense, cybersecurity needs to become a higher priority for election-related infrastructure. The Committee found a wide range of cybersecurity practices across the states. Some states were highly focused on building a culture of cybersecurity; others were severely under-resourced and relying on part-time help.

(U) The Committee recommends State officials work with DHS to evaluate the security of their election systems end-to-end and prioritize implementing the following steps to secure voter registration systems, state records, and other pre-election activities. The Committee additionally recommends that State officials:

---

[370] (U) SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p.15.
[371] (U) DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.
[372] (U) SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p 15, 26.
[373] (U) SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p.113.

- (U) Identify the weak points in their networks, like under-resourced localities. State 7 said they are not worried about locations like larger counties when it comes to network security, but they are worried about "the part-time registrar who is also the town attorney and the town accountant and is working out of a 17th century jail." [374]

- (U) Undertake security audits of state and local voter registration systems, ideally utilizing private sector entities capable of providing such assistance. State and local officials should pay particular attention to the presence of high severity vulnerabilities in relevant web applications, as well as highly exploitable vulnerabilities such as cross-site scripting and SQL injection.

- (U) Institute two-factor authentication for user access to state databases.

- (U) Install monitoring sensors on state systems. As of mid-2018, DHS's ALBERT sensors covered up to 98% of voting infrastructure nationwide, according to Undersecretary Krebs.[375]

- (U) Include voter registration database recovery in state continuity of operations plans.

- (U) Update software in voter registration systems. One state mentioned that its voter registration system is more than ten years old, and its employees will "start to look for shortcuts" as it gets older and slower, further imperiling cybersecurity.

- (U) Create backups, including paper copies, of state voter registration databases.

- (U) Consider a voter education program to ensure voters check registration information well prior to an election.

(U) DHS in the past year has stepped up its ability to assist the states with some of these activities, but DHS needs to continue its focus on election infrastructure and pushing resources to the states.

(U) **The Committee recommends DHS take the following steps**:

- (U) Create an advisory panel to give DHS expert-level advice on how states and localities run elections. The Government Coordinating Council, created as part of the critical infrastructure designation, could serve as a venue for educating DHS on what states do and what they need.

---

[374] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.
[375] (U) DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.

- (U) Create guidelines on cybersecurity best practices for elections and a public awareness campaign to promote election security awareness, working through EAC, NASS, and NASED, and with the advisory panel.

- (U) Develop procedures and processes to evaluate and routinely provide guidance on relevant vulnerabilities associated with voting systems in conjunction with election experts.

- (U) DHS has already created a catalog of services they can provide to states to help secure states' systems. DHS should maintain the catalog and continue to update it as it refines its understanding of what states need.

- (U) Expand capacity so wait times for services, like voluntary vulnerability assessments, are manageable and so that DHS can maintain coverage on other critical infrastructure sectors. Robbing resources from other critical infrastructure sectors will eventually create unacceptable new vulnerabilities.

- (U) Work with GSA to establish a list of approved private-sector vendors who can provide services similar to those DHS provides. States report being concerned about "vultures" —companies who show up selling dubious cyber solutions. That being said, some states will be more comfortable having a private sector entity evaluate their state systems than a federal agency.

- (U) Continue to build the resources of the newly established EI-ISAC. States have already found this information sharing service useful, and it could serve as a clearinghouse for urgent threat information. As of August 2018, the EI-ISAC had over 1,000 members with participants in all 50 states.[376]

- (U) Continue training for state and local officials, like the table-top exercise conducted in August of 2018 that brought together representatives from 44 states, localities, and the federal government to work through an election security crisis.[377] The complexity of the scenario encouraged state and local officials to identify serious gaps in their preparations for Election Day.

5. (U) Build a Stronger Defense, Part IV: Take Steps to Secure the Vote Itself

(U) Given Russian intentions to undermine the credibility of the election process, states should take urgent steps to replace outdated and vulnerable voting systems. When safeguarding the integrity of U.S. elections, all relevant elements of the government—including at the federal, state, and local level—need to be forward looking and work to address vulnerabilities before they are exploited.

---

[376] (U) DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.
[377] (U) DHS, Press release: DHS Hosts National Exercise on Election Security, August 15, 2018.

- **(U)** As states look to replace HAVA-era machines that are now out of date, they should purchase more secure voting machines. Paper ballots and optical scanners are the least vulnerable to cyber attack; at minimum, any machine purchased going forward should have a voter-verified paper trail and remove (or render inert) any wireless networking capability.

- **(U)** States should require that machines purchased from this point forward are either EAC certified or comply with the VVSG standards. State purchasers should write contracts with vendors to ensure adherence to the highest security standards and to demand guarantees the supply chains for machines are secure.

- **(U)** In concert with the need for paper ballots comes the need to secure the chain of custody for those ballots. States should reexamine their safeguards against insertion of fraudulent paper ballots at the local level, for example time stamping when ballots are scanned.

- **(U)** Statistically sound audits may be the simplest and most direct way to ensure confidence in the integrity of the vote.[378] States should begin to implement audits of election results. Logic and accuracy tests of machines are a common step, but do not speak to the integrity of the actual vote counting. Risk-limiting audits, or some similarly rigorous alternative, are the future of ensuring that votes cast are votes counted. State 8, State 12, State 21, State 9, State 2, State 16, and others already audit their results, and others are exploring additional pilot programs.[379] However, as of August 2018, five states conducted no post-election audit and 14 states do not do a complete post-election audit.[380] The Committee recognizes states' concern about the potential cost of such audits and the necessary changes to state laws and procedures; however, the Committee believes the benefit of having a provably accurate vote is worth the cost.

- **(U)** States should resist pushes for online voting. One main argument for voting online is to allow members of the military easier access to their fundamental right to vote while deployed. While the Committee agrees states should take great pains to ensure members

---

[378] **(U)** Election experts point out, however, that audits could create a new vector for election-related lawsuits. Complainants could allege that the audit was done improperly, or that the audit process reflected bias.

[379] **(U)** State 8 passed a law to audit starting in 2018, with random precinct sampling. State 12 does state-wide audits. State 21 audits 2% of ballots, randomly selected. State 9 picks 210 of 4100 precincts at random for an audit. State 2 hand-counts ballots in randomly selected precincts and uses automated software to test. A States law on ballot storage can't accommodate risk-limiting audits. Instead, they use ClearBallot software. They upload images of ballots to an external hard drive and send it to ClearBallot. ClearBallot is blind to who won and independently evaluates the results. In addition, the company can identify problems with scanners; for example, when a fold in absentee ballots recorded as a vote. Cybersecurity experts still doubt, however, that this type of procedure is secure.

[380] **(U)** DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.

of the military get to vote for their elected officials, no system of online voting has yet established itself as secure.[381]

- **(U)** DHS should work with vendors of election equipment to educate them about the vulnerabilities in both the machines and the supply chains for the components of their machines. Idaho National Lab is already doing some independent work on the security of a select set of voting machines, developing a repeatable methodology for independently testing the security of such systems.

- **(U)** The Department of State should work with FBI and DHS to warn states about foreign efforts to access polling places outside normal channels in the future and remain vigilant about rejecting aberrant attempts.

- **(U)** The Associated Press is responsible for reporting unofficial, initial election results on election night and is a critical part of public confidence in the voting tally. States and DHS should work with the AP and other reporting entities to ensure they are both secure and reporting accurate results.

- **(U)** The Committee found that, often, election experts, national security experts, and cybersecurity experts are speaking different languages. Election officials focus on transparent processes and open access and are concerned about introducing uncertainty into the system; national security professionals tend to see the threat first. Both sides need to listen to each other better and to use more precise language.

6. (U) Assistance for the States

(U) State officials told the Committee the main obstacle to improving cybersecurity and purchasing more secure voting machines is cost. State budgets are stretched thin by priorities that seem more urgent on a daily basis and are far more visible to constituents.

(U) In March 2018, Congress appropriated $380 million in funds under the HAVA formula for the states. As of August 2018, states had begun to allocate and spend that money for items such as cybersecurity improvements.

(U) The Committee recommends the EAC, which administers the grants, regularly report to Congress on how the states are using those funds, whether more funds are needed, and whether states have both replaced outdated voting equipment and improved

---

[381] (U) Dr. Halderman in his testimony before the Committee said, "I think that online voting, unfortunately, would be painting a bullseye on our election system. Today's technology just does not provide the level of security assurance for an online election that you would need in order for voters to have high confidence. And I say that having myself . . . hacked an online voting system that was about to be used in real elections, having found vulnerabilities in online voting systems that are used in other countries. The technology just isn't ready for use." *See* SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 152.

cybersecurity. More funds may be needed, as the allocation under the HAVA formula did not prioritize replacing vulnerable electronic-only machines.

- **(U)** States should be able to use grant funds to improve cybersecurity in a variety of ways, including hiring additional IT staff, updating software, and contracting with vendors to provide cybersecurity services. "Security training funded and provided by a federal entity such as the EAC or DHS would also be beneficial in our view,"[382] an official from Illinois testified.

- **(U)** Funds should also be available to defray the cost of instituting audits.

- **(U)** States with vulnerable DRE machines with no paper backup should receive urgent access to funding. Dr. Halderman testified that replacing insecure paperless voting machines nationwide would cost $130 to $400 million dollars. Risk-limiting audits would cost less than $20 million a year.[383]

7. [redacted] **Build a Credible** [redacted]

[redacted]

[redacted]

[382] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 114.
[383] **(U)** *Ibid.*, p. 119.

MINORITY VIEWS OF SENATOR WYDEN

(U) The role of the federal government

(U) The Committee report describes Russian attacks on U.S. election infrastructure in 2016 and lays out many of the serious vulnerabilities that exist to this day. These vulnerabilities pose a direct and urgent threat to American democracy which demands immediate congressional action. The defense of U.S. national security against a highly sophisticated foreign government cannot be left to state and county officials. For that reason, I cannot support a report whose top recommendation is to "reinforce[ ] state's primacy in running elections."

(U) Congress's constitutional role in regulating federal elections is well-established. In response to an inquiry from the bipartisan leadership of the U.S. Senate, the General Accounting Office (GAO) wrote that "[w]ith regard to the administration of federal elections, Congress has constitutional authority over both congressional and presidential elections."[1] Indeed, pursuant to the Elections Clause of the U.S. Constitution,[2] Congress's authority over congressional elections is "paramount to that of the states." As the GAO report details, Congress has repeatedly passed legislation related to the administration of elections on topics such as the timing of federal elections, voter registration, absentee voting requirements, disability access, and voting rights.

(U) If there was ever a moment when Congress needed to exercise its clear constitutional authorities to regulate elections, this is it. America is facing a direct assault on the heart of our democracy by a determined adversary. We would not ask a local sheriff to go to war against the missiles, planes and tanks of the Russian Army. We shouldn't ask a county election IT employee to fight a war against the full capabilities and vast resources of Russia's cyber army. That approach failed in 2016 and it will fail again. The federal government's response to this ongoing crisis cannot be limited offers to provide resources and information, the acceptance of which is voluntary. If the country's elections are to be defended, Congress must also establish mandatory, nation-wide cybersecurity requirements.

(U) Security of voting machines

(U) Experts are clear about the measures necessary to protect U.S. elections from cyber manipulation.[3] Absent an accessibility need, most voters should hand-mark paper ballots. For voters with some kind of need, ballot marking devices that print paper ballots should be available. Risk-limiting audits must be also be required. Currently, however, only Virginia, Colorado and Rhode Island meet these requirements.[4] These critical reforms must be adopted

---

[1] "Elections. The Scope of Congressional Authority in Election Administration," General Accounting Office, March 2001, prepared in response to a joint inquiry from Senator Trent Lott, Republican Leader; Senator Tom Daschle, Democratic Leader; Senator Mitch McConnell, Chairman, and Senator Christopher Dodd, Ranking Member, of the Senate Committee on Rules and Administration.

[2] Article I, Section 4, Clause 1

[3] Securing the Vote; Protecting American Democracy; National Academy of Sciences, Engineering and Medicine, September 2018

[4] National Conference of State Legislatures, Post-Election Audits, January 3, 2019. Verifiedvoter.org. The Verifier – Polling Place Equipment – November 2018. Oregon requires paper ballots and the Oregon State Senate has passed a bill requiring risk-limiting audits.

throughout the country, which is why, on June 27, 2019, the House of Representatives passed H.R. 2722, the Securing America's Federal Elections (SAFE) Act. The security of the country's voting machines depends on this legislation being signed into law.

(U) The Committee, in recommending basic security measures like paper ballots and audits, notes that there is currently "a wide range of cybersecurity practices across the states." Indeed, the data is deeply concerning and highlights the need for mandatory, nation-wide standards. For example, the Committee rightly highlights the vulnerabilities of Direct-Recording Electronic (DRE) Voting Machines, noting that, without a paper trail, there would be no way to conduct a meaningful "recount" and compromises would remain undetected. As of November 2018, however, there were still four states in which every single county relied on DREs without voter verified paper audit trail printers (VVPAT) and, in an additional eight states, there were multiple counties that relied on DREs without a VVPAT.[5] Gaps in the deployment of VVPATs, which are far less secure than hand-marked paper ballots, demonstrate that even bare minimum security best practices are not being met in many parts of the country.

(U) In addition, 16 states have no post-election audits of any kind, while many others have insufficient or perfunctory audits. Only four states have a statutory requirement for risk-limiting audits, while two states provide options for counties to run different kinds of audits, one of which is a risk-limiting audit.[6] Next year, a third state will provide that option. In other words, the vast majority of states have made no moves whatsoever toward implementing minimum standards that experts agree are necessary to guarantee the integrity of elections.

(U) The Committee rightly identifies problems with vendors of voting machines, noting vulnerabilities in both the machines and the supply chains for machine components. Currently, however, the federal government has no regulatory authority that would require these vendors to adhere to basic security practices.[7] Only general federal requirements that states and localities use paper ballots and conduct audits will ensure that the risk posed by voting machines provided by private vendors to states and localities can be contained. The stakes could not be more clear. As Homeland Secretary Kirstjen Nielsen testified to the Committee, "If there is no way to audit the election, that is absolutely a national security concern."[8]

(U) Registration databases and election night reporting websites

(U) Two additional components of the U.S. election infrastructure require immediate, mandatory cybersecurity fixes. The first are voter registration databases. The Committee received testimony about successful Russian exfiltration of databases of tens of thousands of voters.[9] Expert witnesses also described the chaos that manipulated voter registration data could cause should voters arrive at the polls and find that their names had been removed from the rolls.

---

[5] Verifiedvoter.org. The Verifier – Polling Place Equipment – November 2018.
[6] The four states are Colorado, Nevada, Rhode Island, and Virginia. National Conference of State Legislatures. Post-Election Audits, January 3, 2019.
[7] Testimony of Homeland Security Secretary Kirstjen Nielsen, March 21, 2018.
[8] Testimony of Homeland Security Secretary Kirstjen Nielsen, March 21, 2018.
[9] Testimony of Connie Lawson, President-elect, National Association of Secretaries of State, and Secretary of State, State of Indiana; testimony of Steve Sandvoss, Executive Director of Illinois State Board of Elections, June 21, 2017; Illinois Voter Registration System Database Breach Report.

As one expert testified, this form of interference "could be used to sabotage the election process on Election Day."[10]

(U) The Committee report describes a range of cybersecurity measures needed to protect voter registration databases, yet there are currently no mandatory rules that require states to implement even minimum cybersecurity measures. There are not even any voluntary federal standards.

(U) An additional component of the U.S. election infrastructure that requires immediate, mandatory cybersecurity measures are the election night reporting websites run by the states. The Committee heard testimony about a Russian attack on Ukraine's web page for announcing results. That attacked allowed the Russians to use misinformation that left Ukraine in chaos for days after the election. As the Committee's expert witness warned, "[w]e need to look at that playbook. They will do it to us."[11] Like voter registration databases, election results websites are not subject to any mandatory standards. Both of these critical vulnerabilities, as well as vulnerabilities of voting machines, must be addressed by the U.S. Congress through the passage of S. 2238, the Senate version of the SAFE Act.

(U) Given the inconsistent, and at times non-existent adherence to basic cybersecurity among states and localities, I cannot agree with the Committee's conclusion that "the country's decentralized election system can be a strength from a cybersecurity perspective." Until election security measures are required of every state and locality, there will be vulnerabilities to be exploited by our adversaries. The persistence of those vulnerabilities has national consequences. The manipulation of votes or voter registration databases in any county in the country can change the result of a national election. The security of the U.S. election system thus hinges on its weakest links – the least capable, least resourced local election offices in the country, many of which do not have a single full-time employee focused on cybersecurity.

(U) Every American has a direct stake in the cybersecurity of elections throughout the country. Congress has an obligation to protect the country's election system everywhere. If there were gaps in the defense of our coastline or air space, members would ensure that the federal government close them. Vulnerabilities in the country's election cybersecurity require the same level of national commitment.

(U) Cybersecurity vulnerabilities and influence campaigns

(U) The cybersecurity vulnerabilities of the U.S. election system cannot be separated from Russia's efforts to influence American voters. As the January 2017 Intelligence Community Assessment (ICA) concluded, and as the Committee report notes, the Russians were "prepared to publicly call into question the validity of the results" and "pro-Kremlin bloggers had prepared a Twitter campaign, #DemocracyRIP, on election night in anticipation of Secretary Clinton's victory." This plan highlights an additional reason why nation-wide election cybersecurity standards are so critical. If Russia's preferred candidate does not prevail in the 2020 election, the

[10] Testimony of Alex J. Halderman, Professor of Computer Science and Engineering, University of Michigan, June 21, 2017.
[11] Testimony of Eric Rosenbach, Co-Director of the Belfer Center for Science and International Affairs, Harvard Kennedy School, March 21, 2018.

Russians may seek to delegitimize the election. The absence of any successful cyber intrusions, exfiltrations or manipulations would greatly benefit the U.S. public in resisting such a campaign.

(U) While not formally part of the U.S. election infrastructure, the devices and accounts of candidates and political parties represent an alarming vulnerability in the country's overall election system. Russia's campaign of hacking the emails of prominent political figures and releasing them through Wikileaks, Gucifer 2.0, and DCLeaks was probably its most effective means of influencing the 2016 election. The Committee has received extensive testimony about these operations, the vulnerabilities that allowed them to occur, and the threat those vulnerabilities pose to the integrity of American democracy.[12] Yet little has been done to prevent it from happening all over again. S. 1569, the Federal Campaign Cybersecurity Assistance Act of 2019, addresses these vulnerabilities head on by authorizing political committees to provide cybersecurity assistance to candidates, campaigns and state parties.

(U) These vulnerabilities extend to the U.S. Senate, most of whose members are or will be candidates for reelection or for other positions. As a November 2018 Senate report noted, there is "mounting evidence that Senators are being targeted for hacking, which could include exposure of personal data."[13] Private communications and information reside on personal accounts and devices. Passage of S. 890, the Senate Cybersecurity Protection Act, will authorize the Senate Sergeant at Arms to protect the personal devices and accounts of Senators and their staff and help prevent the weaponization of their data in campaigns to influence elections.

(U) Assessments related to the 2016 election

(U) I have also submitted these Minority Views to address assessments related to Russian activities during the 2016 election. According to the January 2017 ICA, DHS assessed that "the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying." An assessment based on observations is only as good as those observations and this assessment, in which DHS had only moderate confidence,[14] suffered from a lack of observable data. As Acting Deputy Undersecretary of Homeland Security for National Protection and Programs Directorate, Jeannette Manfra, testified at the Committee's June 21, 2017, hearing, DHS did not conduct any forensic analysis of voting machines.

(U) DHS's prepared testimony at that hearing included the statement that it is "likely that cyber manipulation of U.S. election systems intended to change the outcome of a national election would be detected." The language of this assessment raises questions, however, about DHS's ability to identify cyber manipulation that could have affected a very close national election, particularly given DHS's acknowledgment of the "possibility that individual or isolated cyber

---

[12] See, for example, Committee hearing, March 30, 2017.
[13] Senators' Personal Cybersecurity Working Group Report, submitted by the Senators' Personal Cybersecurity Working Group, November 2018.
[14] Responses to Questions for the Record from Dr. Samuel Liles, Acting Director of Cyber Division, Office of Intelligence and Analysis; and Jeanette Manfra, Acting Deputy Undersecretary, National Protection and Programs Directorate, following Committee hearing, June 21, 2017.

intrusions into U.S. election infrastructure could go undetected, especially at local levels."[15] Moreover, DHS has acknowledged that its assessment with regard to the detection of outcome-changing cyber manipulation did not apply to state-wide or local elections.[16]

(U) Assessments about manipulations of voter registration databases are equally hampered by the absence of data. As the Committee acknowledges, it "has limited information on the extent to which state and local election authorities carried out forensic evaluation of registration databases." Assessments about Russian attacks on the administration of elections are also complicated by newly public information about the infiltration of an election technology company. Moreover, as the Special Counsel reported, the GRU sent spear phishing emails to "Florida county officials responsible for administering the 2016 election" which "enabled the GRU to gain access to the network of at least one Florida county government."[17]

(U) The Committee, in stating that it had found no evidence that vote tallies were altered or that voter registry files were deleted or modified, rightly noted that the Committee's and the IC's insight into this aspect of the 2016 election was limited. I believe that the lack of relevant data precludes attributing any significant weight to the Committee's finding in this area.

(U) The Committee's investigation into other aspects of Russia's interference in the 2016 election will be included in subsequent chapters. I look forward to reviewing those chapters and hope that outstanding concerns about members' Committee staff access to investigative material, including non-compartmented and unclassified information, will be resolved.

---

[15] Responses to Questions for the Record from Dr. Samuel Liles, Acting Director of Cyber Division, Office of Intelligence and Analysis; and Jeanette Manfra, Acting Deputy Undersecretary, National Protection and Programs Directorate, following.Committee hearing, June 21, 2017.

[16] Responses to Questions for the Record from Dr. Samuel Liles, Acting Director of Cyber Division, Office of Intelligence and Analysis; and Jeanette Manfra, Acting Deputy Undersecretary, National Protection and Programs Directorate, following.Committee hearing, June 21, 2017.

[17] Report on the Investigation Into Russian Interference In The 2016 Presidential Election, Special Counsel Robert S. Mueller III, March 2019

ADDITIONAL VIEWS OF SENATORS HARRIS, BENNET, AND HEINRICH

(U) The Russian government's attack on the 2016 election was the product of a deliberate, sustained, and sophisticated campaign to undermine American democracy. Russian military intelligence carried out a hacking operation targeting American political figures and institutions. The Internet Research Agency—an entity with ties to Russian President Vladimir Putin—used social media to sow disinformation and discord among the American electorate. And, as this report makes clear, individuals affiliated with the Russian government launched cyber operations that attempted to access our nation's election infrastructure, in some cases succeeding.

(U) The Russian objectives were clear: deepen distrust in our political leaders; exploit and widen divisions within American society; undermine confidence in the integrity of our elections; and, ultimately, weaken America's democratic institutions and damage our nation's standing in the world. The Committee did not discover evidence that Russia changed or manipulated vote tallies or voter registration information, however Russian operatives undoubtedly gained familiarity with our election systems and voter registration infrastructure—valuable intelligence that it may seek to exploit in the future.

(U) The Committee's report does not merely document the wide reach of the Russian operation; the report reveals vulnerabilities in our election infrastructure that we must collectively address. We do not endorse every recommendation in the Committee's report, and we share some of our colleagues' concerns about the vulnerability that we face, particularly at the state level, where counties with limited resources must defend themselves against sophisticated nation-state adversaries. Nevertheless, the report as a whole makes an important contribution to the public's understanding of how Russia interfered in 2016, and underscores the importance of working together to defend against the threat going forward.

(U) It is critical that state and local policymakers study the report's findings and work to secure election systems by prioritizing cybersecurity, replacing outdated systems and machines, and implementing audits to identify and limit risk. The Intelligence Community and other federal agencies must improve efforts to detect cyberattacks, enhance coordination with state and local officials, and develop strategies to mitigate threats. And, critically, Congress must take up and pass legislation to secure our elections. We must provide states the funding necessary to modernize and maintain election infrastructure, and we must take commonsense steps to safeguard the integrity of the vote, such as requiring paper ballots in all federal elections.

(U) Our adversaries will persist in their efforts to undermine our shared democratic values. In order to ensure that our democracy endures, it is imperative that we recognize the threat and make the investments necessary to withstand the next attack.

The New York Times https://nyti.ms/2HbyQkU

TUNE IN, TURN OUT

I Hacked an Election. So Can the Russians.

By J. Alex Halderman

April 5, 2018

This video is part of a series on voting in America, which will run until Election Day in November. For more, see:

Part 1: On the importance of voting.
Part 2: On a court case over a Kansas voter registration law.
Part 3: On discriminatory voting laws.

J. Alex Halderman (@jhalderm) is a professor of computer science and engineering at the University of Michigan.